DPS Telecom

"Your Partners in Network Alarm Monitoring"

Web Browser

USER MANUAL

Visit our website at www.dpstelecom.com for the latest PDF manual and FAQs.

January 15, 2005 **D-OC-UM081.15000** **Firmware Version 3.2C**

Revision History	
January 15, 2008	Changed how time zone is set the change was added in NetGuardian v3.2C firmware.

Notice

The material in this manual is for information purposes and is subject to change without notice. DPS Telecom shall not be liable for errors contained herein or consequential damages in connection with the furnishing, performance, or use of this manual.

Contents

Visit our website at www.dpstelecom.com for the latest PDF manual and FAQs

1 Overview

Fig. 1.1 NetGuardian 832A monitors alarms, pings network elements, and reports via SNMP, pager or email.

1.1 Introduction

The NetGuardian's Web Browser interface lets you manage alarms and configure the unit through Internet or Intranet. You can quickly set up alarm point descriptions, view alarm status, issue controls, and configure paging information, as well as additional options. The NetGuardian supports Internet Explorer versions 4.0 and above and Netscape Navigator versions 4.7 and above.

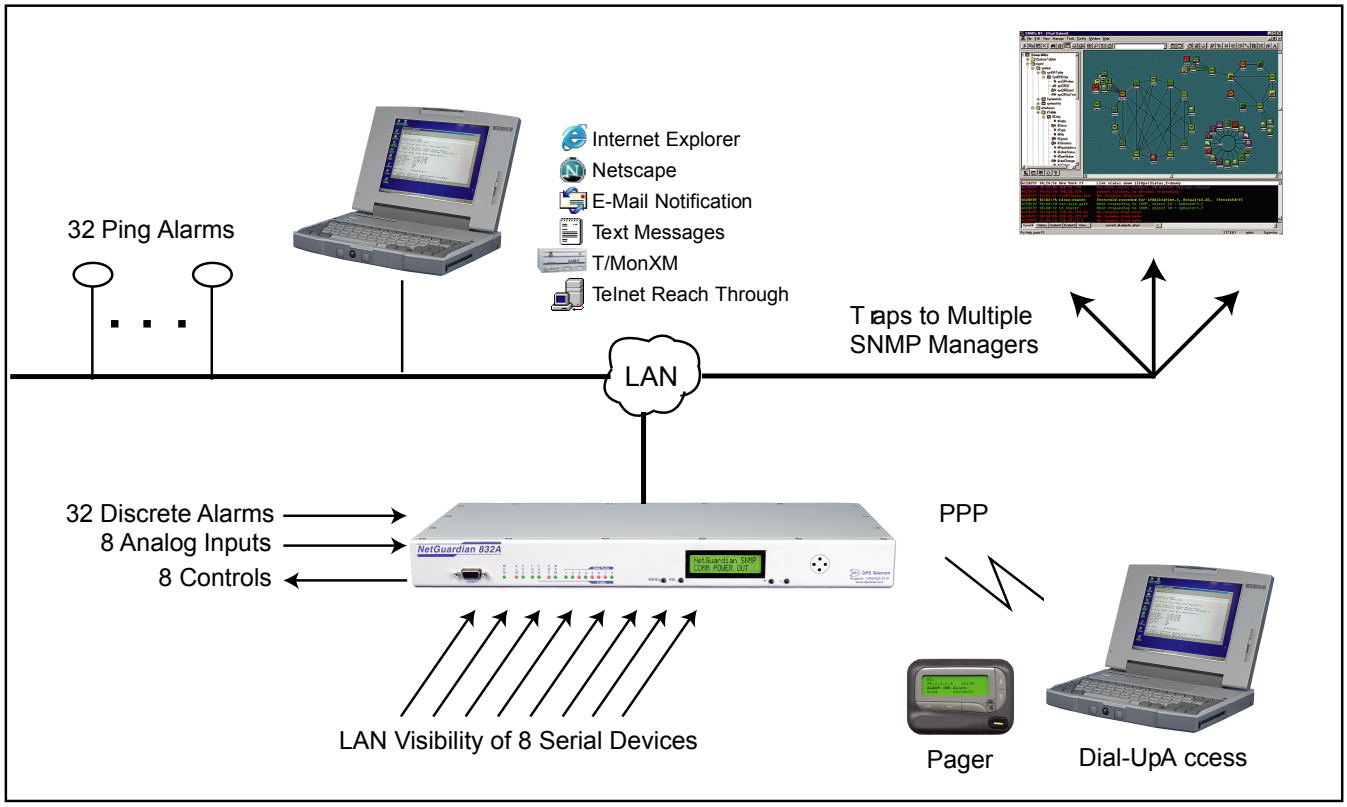


Fig. 1.2 NetGuardian 832A monitors IP aware devices' network presence and also interfaces discrete alarm points and controls at your network sites.

1.2 Potential Problems using Web Interface in a Secure Proxy Network

Using the Web Browser interface for the NetGuardian in a secure proxy network can cause certain problems to occur. If you are logged on to the NetGuardian from within your network through a proxy, and another user from within your network tries to access the same NetGuardian, the second user will not need to login to the NetGuardian. Both users will essentially be logged in using the same IP address because of the masking done by the proxy server.

2 Unit Configuration

2.1 Logging on to the NetGuardian

For web interface functionality, the unit must first be configured with some basic network information. If this step has not been done, refer to the NetGuardian User Manual for Initial Software Configuration setup.

1. To connect to the NetGuardian from your web browser, you must know it's IP address or domain name if it has been registered with your internal DNS. Enter it in the address bar of your web browser (it may be helpful to bookmark the logon page to simplify access).

2. After connecting to the NetGuardian's IP address, enter your password and click Submit. See Fig.2.1.
Note: factory default password is "dpstelecom."

3. In the main menu there is a Monitor menu button and an Edit menu button. Most of the software configuration will occur in the edit menu. The following sections provide detailed information regarding these functions.

Note: If the edit menu does not appear in the left frame after logging on, it means that another station has already logged on as the primary user. The maximum number of users allowed to simultaneously access the NetGuardian via Web Browser is 4, where the primary user is the only user with access to the Editing features. Also, closing out of Explorer without logging out prevents other users from accessing the Editing features. Web Browser sessions are tracked by IP Address and the session will time out after 12 minutes of inactivity.

Fig. 2.1 Enter your password to configure and monitor your NetGuardian using the Web Browser feature.

2.2 Entering System Settings

From the System screen, enter the name, location, contact, features, and SNMP community names (See Figure 2.2 and Table 2.A).
1. From the Edit menu, select "System". See Figure 2.3.
2. Enter the user designated name for your NetGuardian 832A*.
3. Enter the location or address of the NetGuardian 832A*.
4. Set the Contact by entering the telephone number or other contact information for the person or group responsible for this NetGuardian 832A.
5. The Features field is used for entering feature codes for future upgrades.
6. Enter the community name for SNMP GET requests.
7. Enter the community name for SNMP SET requests.
8. Enter the community name for SNMP TRAPs.
*If using email pager type—refer to Section 2.5 for correct name and location field formatting.

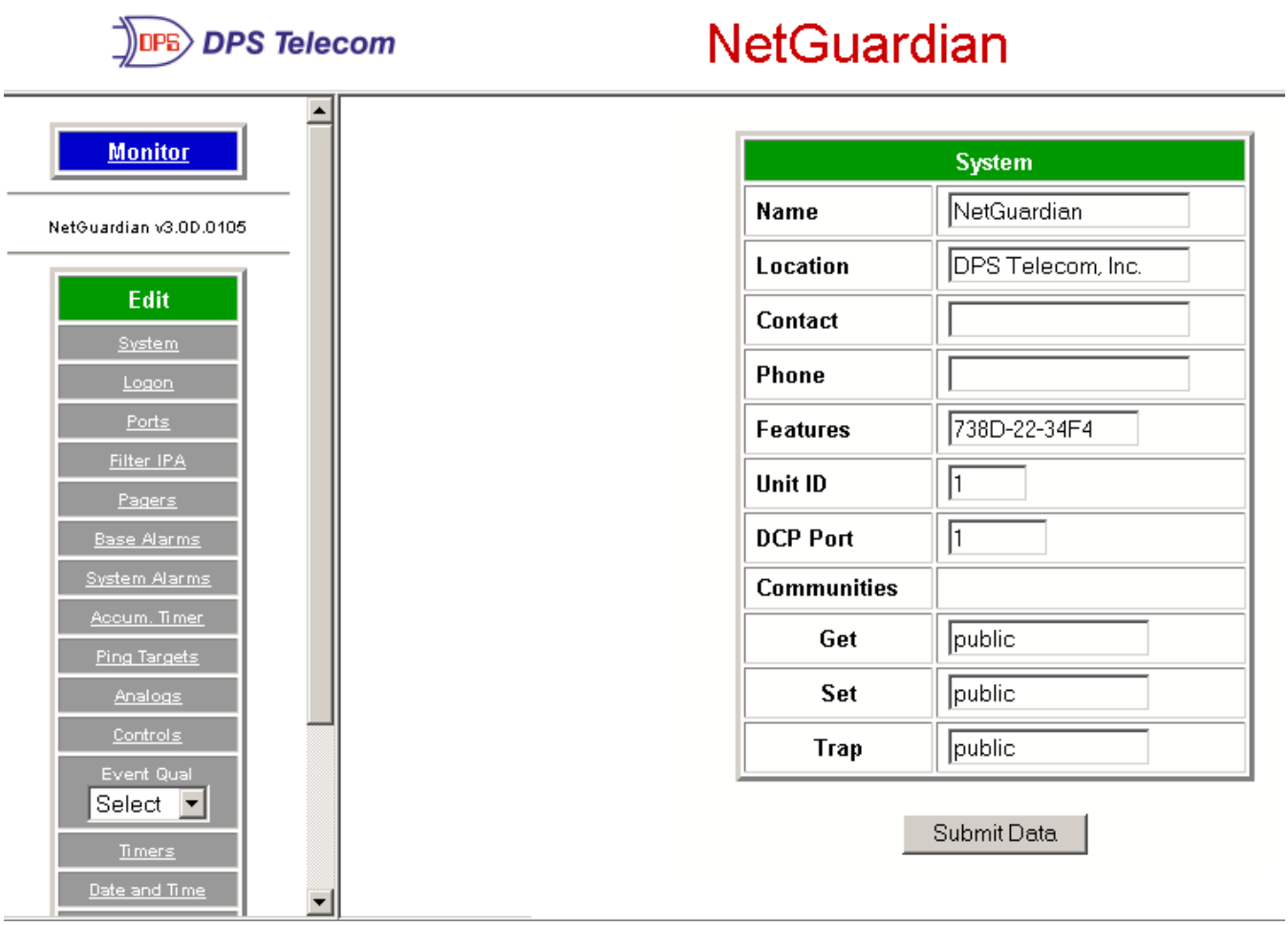


Fig.2.2 Configure the system information by selecting the System screen from the Edit menu.

Field	Description
Name	User designated name for this NetGuardian 832A (also used for portion of "from" address in e-mail notification of alarms).
Location	Location or address of the NetGuardian 832A (also used for portion of "in" address in e-mail notification of alarms).
Contact	Information for how to contact the person responsible for this NetGuardian 832A.
Phone	Contact's telephone number.
Features	Used for entering feature codes for future upgrade features.
Unit ID	User definable ID number for this NetGuardian (DCP Address).
DCP Port	Enter the DCP Port for this NetGuardian.
Analog LCD	Enable or disable display of analog values to the LCD.
Communities	
G)et	Community name for SNMP requests.*
S)et	Community name for SNMP SET requests.*
T)rap	Community name for SNMP TRAP requests.*

Table 2.A. System fields.

2.3 Changing the Logon Password

The password can be configured from the Login - Master Password field. The password must be at least 3 characters long. For security reasons, DPS recommends setting the minimum password length to at least 5 characters. The factory default password is "dpstelecom". The Advanced field gives users the ability to initiate a security dial-back function as well as to enter logon profiles. See Section 2.3.1 for dial-back and logon profile configuration information.

1. From the Edit menu, select "Logon". See Figure 2.3.
2. Enter the minimum password length you wish to set (the minimum length is 3 characters, however, for security reasons, DPS recommends setting the minimum password length to at least 5 characters).
3. Enter your new password in the "Password" and "Confirm Password" fields.
4. Click the "Submit Data" button.

Note: DPS Telecom strongly recommends that the default password be changed.

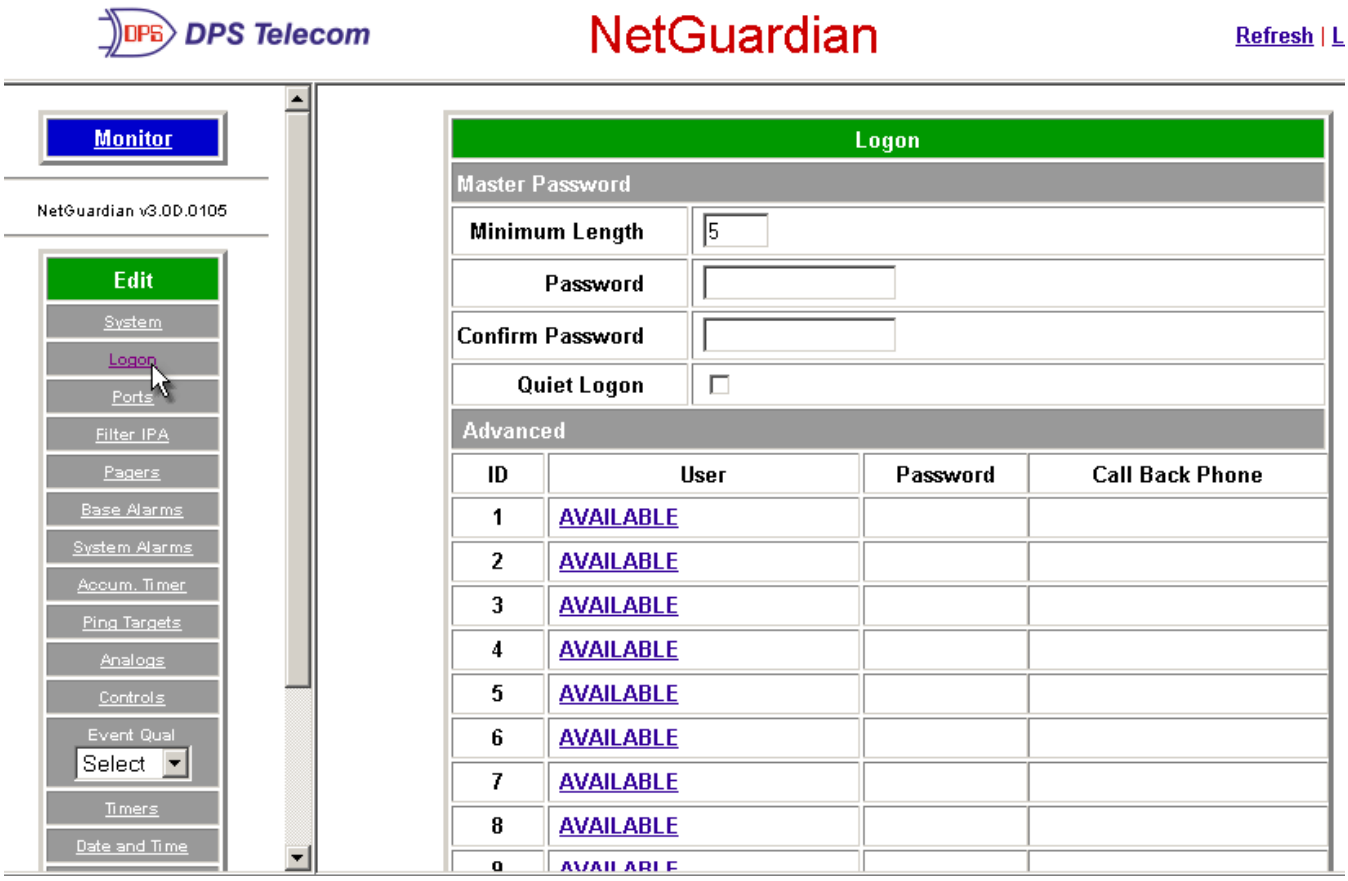


Fig. 2.3 Configure the password parameters from the Login screen.

2.3.1 Security Dial-back and logon profiles

The dial-back feature serves as an additional level of security to the modem, but it also serves to restrict access to the NetGuardian's functions may be granted to individuals. By creating logon profiles, network managers are able to grant personnel access to certain functions of the NetGuardian without allowing access to sensitive or secure areas of the database.

Once users are assigned a logon profile, along with a unique NetGuardian logon password, the unit can be set to initiate a dial-back when a valid logon password is entered. If a valid password is entered, users will see "accepted, Disconnecting". The NetGuardian will then hang up and dial back to the users modem using the

number entered in the logon profile. When the NetGuardian dials back, the user will be logged on to whatever security access that user has been granted in their logon profile.

Note: To enable dial-back security, at least one of the Access Privileges must be activated and a call back phone number must be defined. As long as the dial-back security mode is enabled, that will be the only method of external dialup access to the unit.

1. From the Edit menu select Logon. Click on the "Available" link to configure/add user profiles—refer to Fig. 2.3.
2. Enter the user information in the appropriate fields. See Table 2.B for field and access privileges descriptions.
3. Click Submit Data to save user profile.

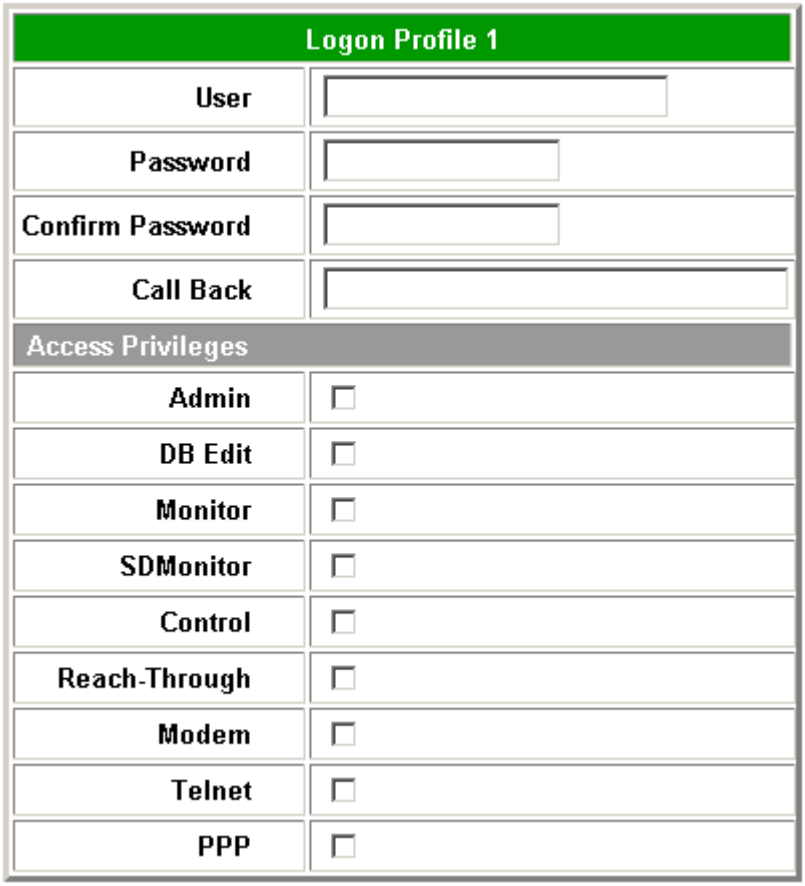


Fig. 2.4 Configure logon profiles by clicking on an available user field.

Profile Field	Description
User	Enter a username or a user description (18 characters max.).
Password	Enter a unique user password (3 character min.). This password will be used by the NetGuardian to determine whether or not to initiate the "Call-Back" function and also if any limited access applies.
Confirm Password	Re-enter the password.
Call Back	This is the number the NetGuardian uses to "call back" to the user's modem.
Access Privileges	
Admin	Enables the user to add/modify logon profiles and NetGuardian password information. Selecting security also automatically activates DB Edit.
DB Edit	Enables the user to perform data base edits in the NetGuardian.
Monitor	Enables the user to have Monitor access of the NetGuardian.
SDMonitor	Enables the user to view seral port buffers.
Control	Gives the user the ability to issue controls. This also automatically activates Monitor and DB Edit.
Reach-Through	Enables the user to achieve reach-through (Proxy) access.
Modem	Enables the user to call in to the unit.
Telnet	Enables the user to have Telnet access to the unit.
PPP	Enables the user to access the PPP server with the user defined password.

Table 2.B Logon profile field descriptions.

2.4 Configuring Port Parameters

The Ports menu allows you to configure the Ethernet, Modem, Craft port and Data port settings.

2.4.1 Ethernet Ports

1. From the Edit menu, select "Ports"—see Figure 2.5.
2. Unit Address - IP address of the NetGuardian.
3. Subnet Mask - A road sign to the NetGuardian 832A telling it whether your packets should stay on your local network or be forwarded somewhere else on a wide area network.
4. Default Gateway - An important parameter if you are on a network that is connected to a wide area network. It tells NetGuardian 832A which machine is the gateway out of your local network. Set to 255.255.255.255 if not using.
5. DNS Address - IP address of the domain name server.
6. Trap Address - Defines the SNMP Trap Manager's IP address.
7. SNMP Port - The SNMP port is the UDP port set by the SNMP manager to receive traps, usually set to 162.
8. Proxy Base - Defines the NetGuardian TCP ports used by data ports 1-8 (serial ports). Data port 1 receives the port number entered here. Data ports 2-8 receive the next 7 port numbers in ascending order. (i.e. TCP port 3000 through port 3007 at the IP address of the NetGuardian).
9. DHCP - Toggles the Dynamic Host Connection Protocol On or Off.
10. Base URL - The Base URL is the destination website address of the alarm point descriptions hyperlinks. See Section 2.4.2 (Creating Links) for more information.
11. MAC Address: Hardware address of the NetGuardian.

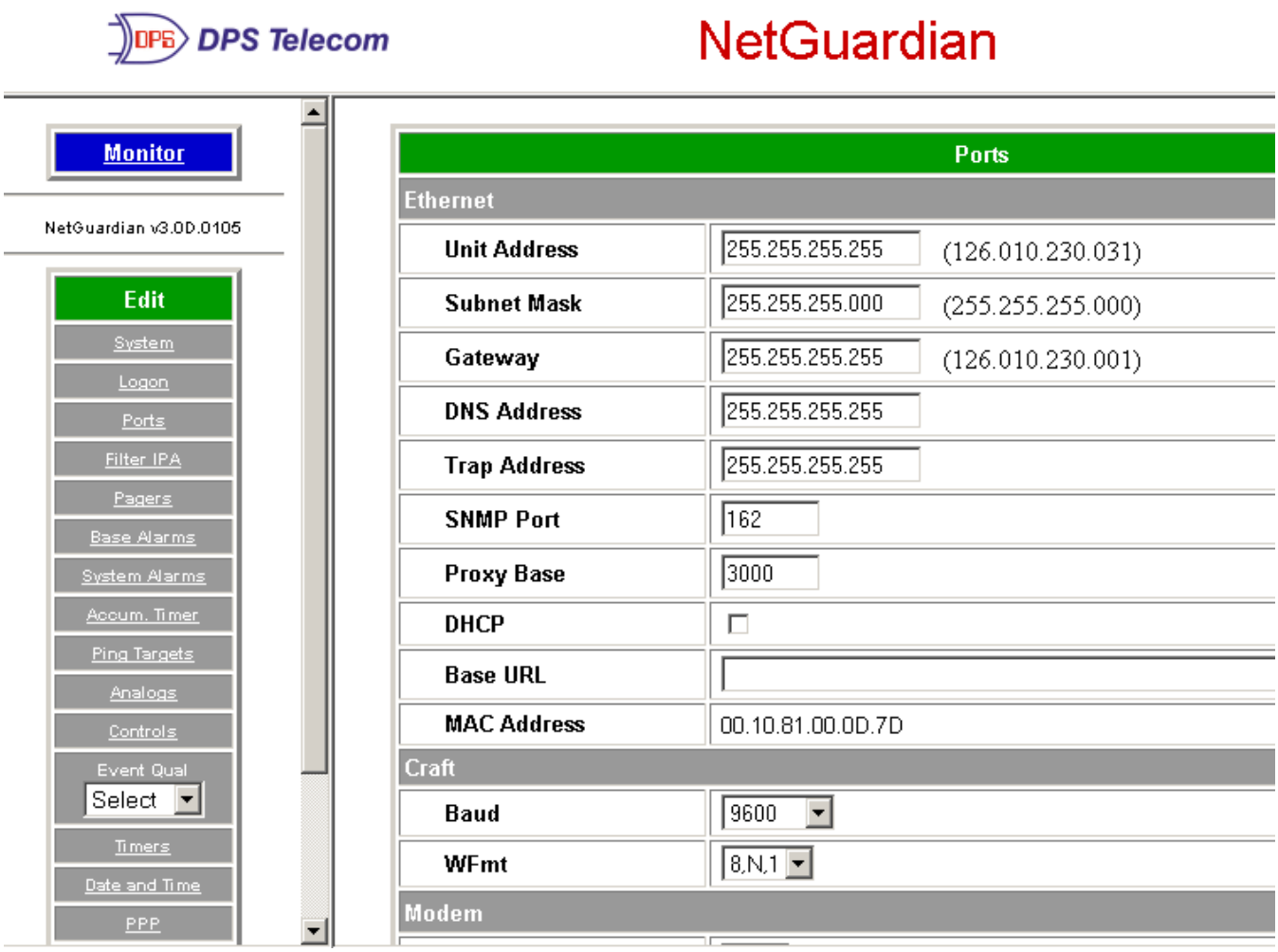


Fig. 2.5 All port configuration is accomplished from the Edit-Ports window.

2.4.2 Using the Base URL Field

The NetGuardian 832A allows users to turn each alarm point description into a hyperlink. When utilized, the alarm description for each alarm point that appears in the monitor mode (for Base Alarms, Ping Targets, or System Alarms) becomes a link that directs technicians/managers to specific web pages or to other files viewable via a Web Browser. This allows users to create easily accessible informational databases on how to handle specific alarm conditions or other instructions. The hyperlinked page or file will be displayed in the main window frame of the NetGuardian Web Browser.

Follow the directions below to create hyperlinks for alarm point descriptions.

1. From the Edit Menu select Ports. Scroll down to the Base URL field—refer to Fig. 2.5.

2. Enter your base URL (e.g. http://www.dpstele.com). The NetGuardian creates the links from the alarm point descriptions based on the URL. Once the base URL is entered, the NetGuardian automatically attaches a unique suffix to each alarm point. For example, if the base URL is "http://www.dpstele.com", the link for the Base Alarm at point 1 would be "http://www.dpstele.com/base1.html"—base Alarm point 2 would be "http://www.dpstele.com/base2.html", and so on.

3. To add a suffix other than "html" to the hyperlinks, insert the text "&pntID;" into the base URL. This allows the user to specify the extension. For example if the base URL is "http://www.dpstele.com/&pntID;.pdf", the link for the Base Alarm at point 1 would be "http://www.dpstele.com/base1.pdf/". Any file type that is

viewable in your Web Browser (e.g. word document, PDF, txt, etc.) is a linkable file.

4. The same link structure applies to the Ping Alarms, System Alarms, and Analog Alarms fields. See Table 2.C for specific URL extension link information.

Alarm Page	Base URL web page link*
Base Alarms	Base1.html – base32.html
Ping Alarms	Ping1.html – ping32.html
System Alarms	System1.html – system64.html
Analog Alarms	Analog1.html – analog8.html

Table 2.C Specific link extensions.

* Using the "&pntID;" code in the base URL enables you to link to any file type viewable in your Web Browser.

2.4.3 Filter IPA Config and Operation

The Filter IPA table allows the user to increase the NetGuardian's network security by allowing packets from specified addresses. Addresses which appear in the table will be processed by the NetGuardian. Defined addresses associated with network cameras or the network time server are automatically processed and will not be filtered out by this feature. Broadcast packets of 255.255.255.255 and ARP requests for the NetGuardian IP address are also not filtered.

1. From the edit menu on the left hand menu frame, select "Filter IPA".
2. The warning prompt will appear. Click OK to continue or exit to cancel.
3. Once enabled, only the IP addresses in the table will be allowed access to the NetGuardian.
4. Select to "Enable IPA Table".
5. Enter the IP address of the machine(s) you would like to give access to the NetGuardian.
6. Entering a zero in any of the octet fields will declare that part of the octet to be a wildcard.

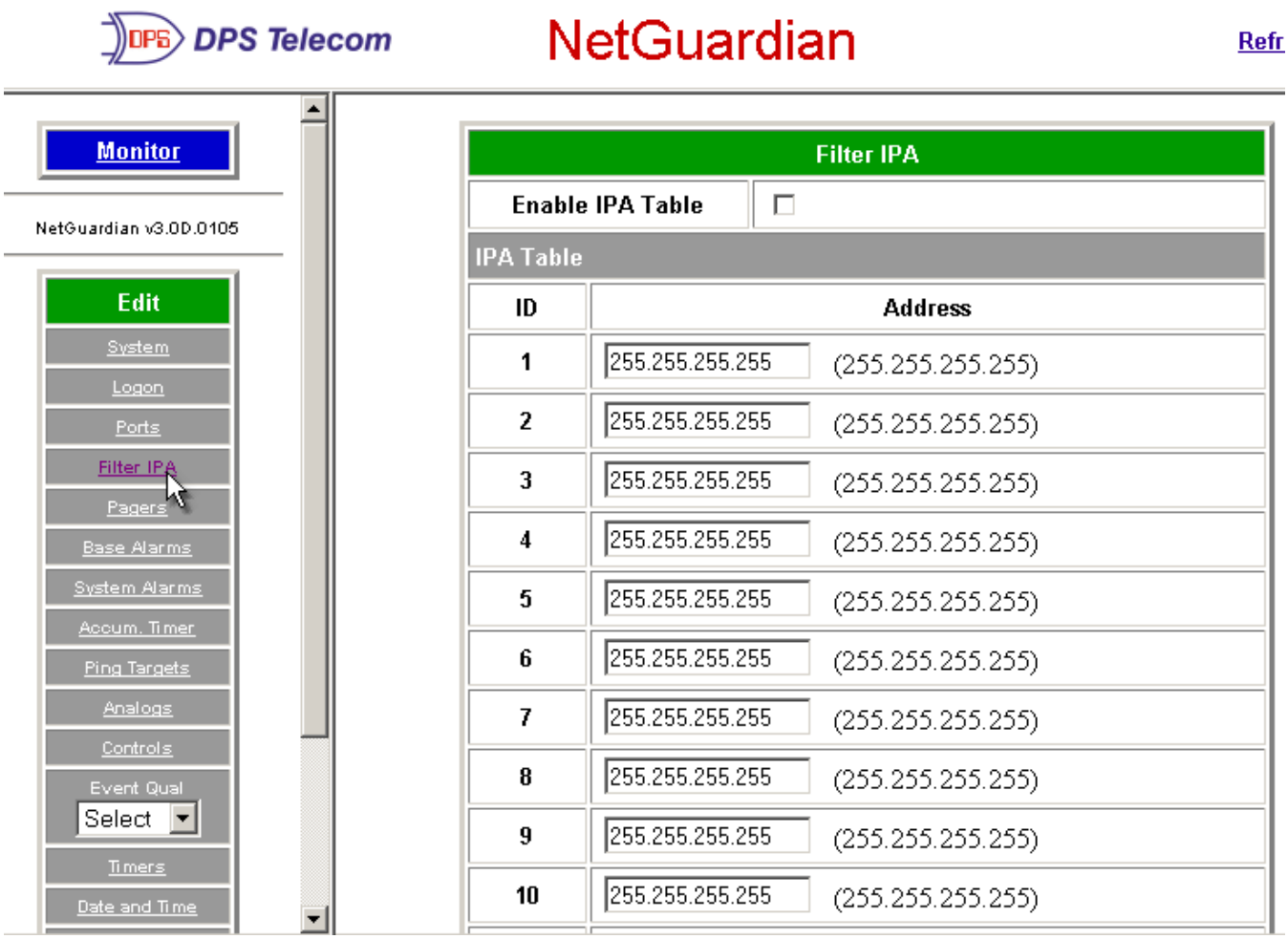


Fig. 2.5 Select Filter IPA from the Edit menu to configure your Filter IPA table.

2.4.4 Changing Craft Port Communication Settings

1. From the "Ports" window, scroll down until you see the "Craft" section—see Figure 2.6.
2. You can set the Baud rate for the craft port to 300, 1200, 2400 or 9600. (Default Baud is 9600)
3. Under the Wfmt (word format) field, select the appropriate Data Bits, Parity, Stop Bits setting to match your terminal emulation software or device connected to the NetGuardian craft port (Default designation is 8,N,1).

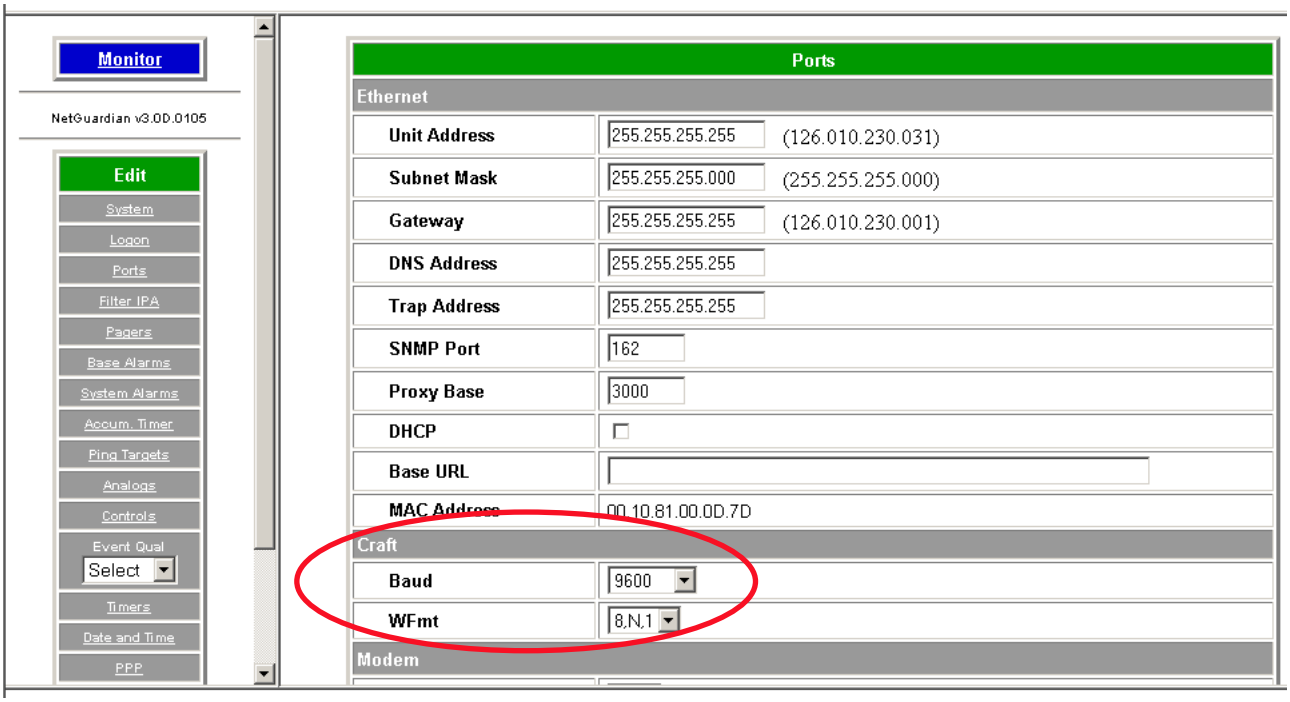


Fig. 2.6 Configure the front panel Craft Port parameters from the Ports screen.

2.4.5 Configuring Modem Port Settings

1. From the "Ports" window, scroll down until you see the "Modem" section—see Figure 2.5.
2. Set the Ring Count. This parameter defines the number of rings before answering (Default = 1).
3. The "Dial Init" and the "Answer Init" fields can be used if any other modem initialization settings need to be set. For example, the modem can be set to ignore the dial-tone by entering a character code in either the Answer Init (in to the NetGuardian) or the Dial Init (out from the NetGuardian)—refer to a standard modem command (Hayes) reference book for standard commands. The default setting for these fields is blank (N/A).

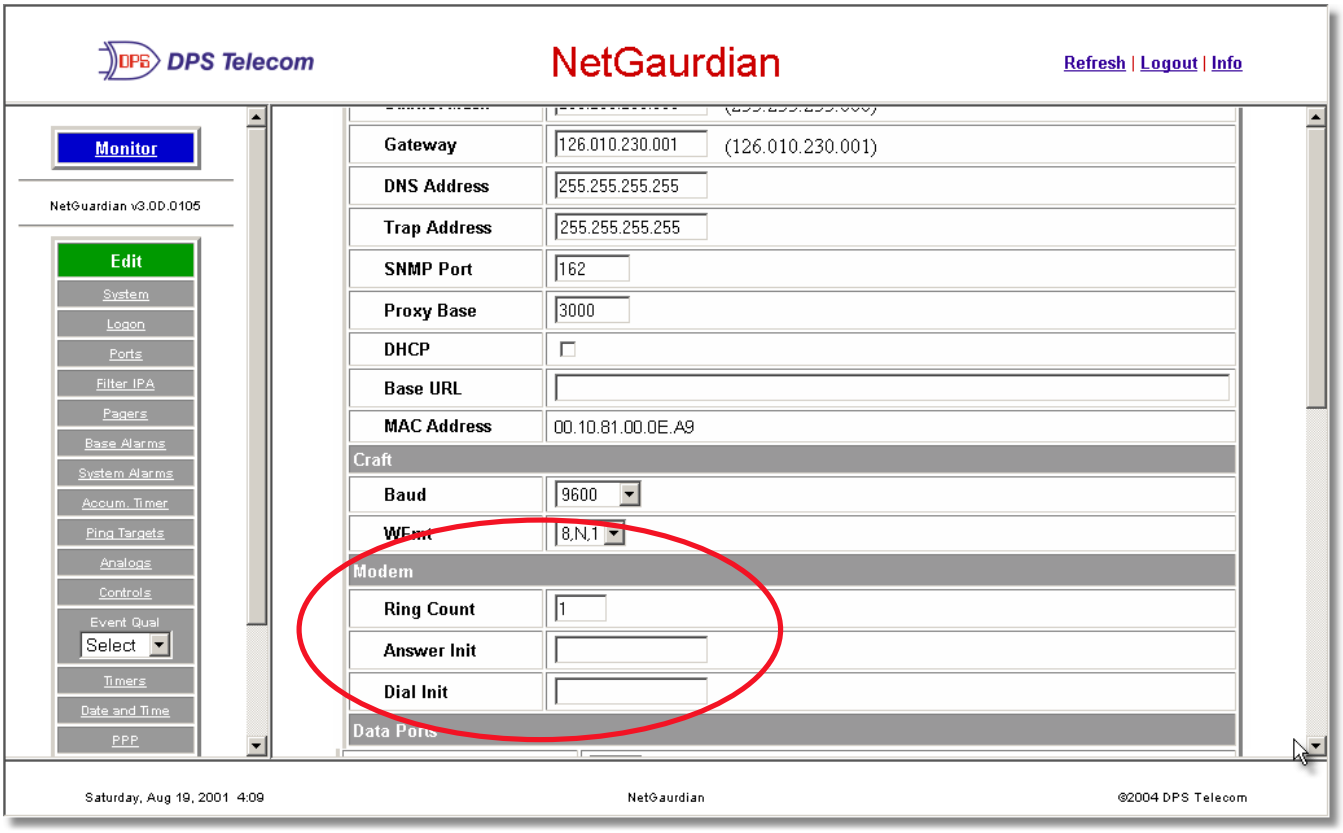


Fig. 2.5 Change the Modem Settings from the Edit > Ports screen.

2.4.6 Configuring Data Ports 1 - 8

1. From the "Ports" window, scroll down until you see the "Data Ports" section—see Figure 2.6.
2. Under the options heading, enter in the appropriate number of GLDs (1-12) or NetGuardian Discrete Expansions (1-3) installed*. Entering zero disables these options. If connecting more than 3 GLDs, the baud rate must be set to 9600.
3. Enter a description for each port with a connected device. The communication settings for each port can be configured for Baud rate**, word format and to ignore or remove CR/LF (carriage return/line feed) characters in either the input or output data stream.
4. Refer to Table 2.D to select the correct port type setting for your application.

*GLDs use port 8 and NetGuardian Expansions use port 7. See their respective user manuals for detailed configuration information.
**The baud rate for the bridged channel pairs (see Table 2.D for description) may be set in any combination except 19200 and 38400.

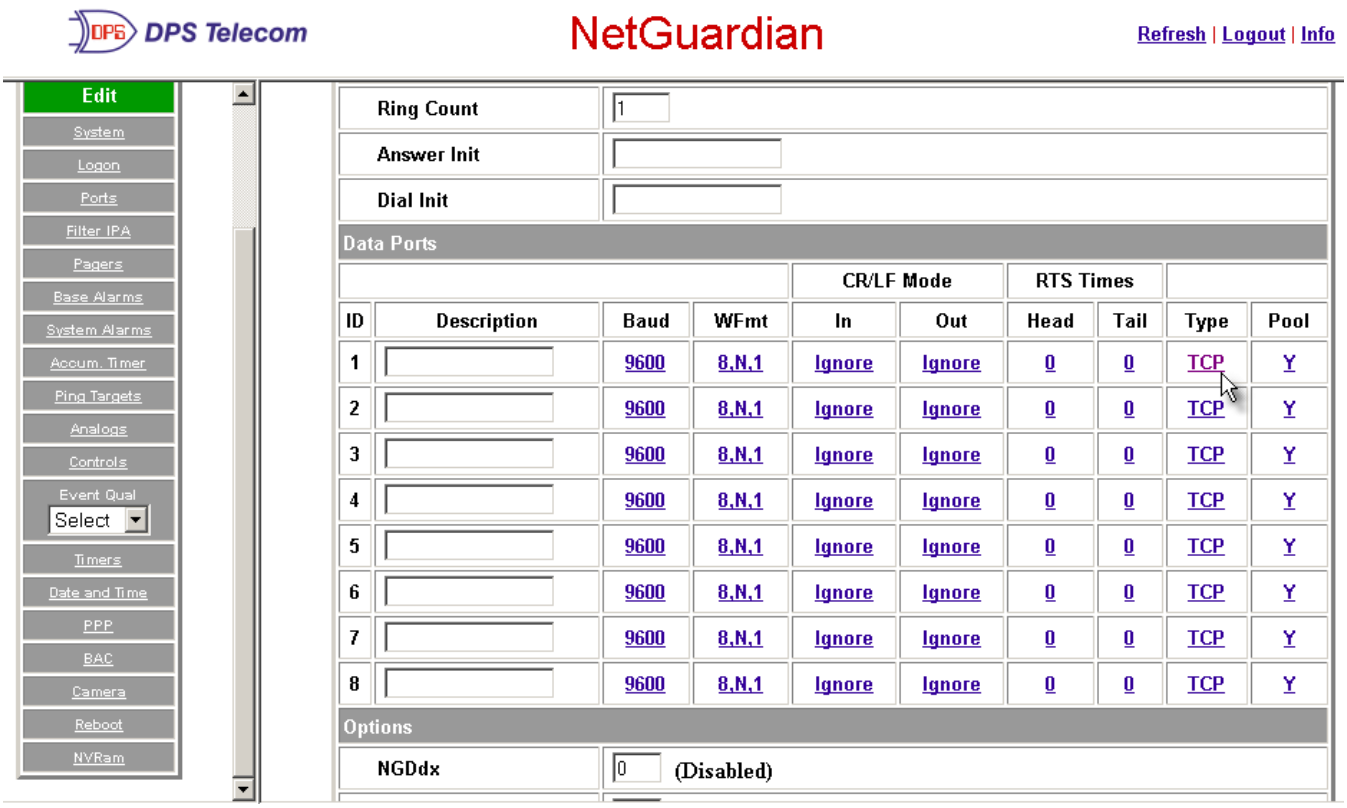


Fig. 2.6 Configure the Data Port parameters from the Ports screen.

Type	Description
TCP	Makes reach-through available at TCP ports (Telnet).
RTCP	Raw TCP (negates Telnet negotiation).
HTCP	High speed TCP port (only 1 HTCP port is available).
PTCP	Permanent TCP (during a proxy connection, the connection will never time out).
SPS8	Serial Port Switch 8 (allows eight serial devices to be connected to single port).
UDP	Makes reach-through available at UDP ports (reserved for future use).
CHAN	Creates logical bridge to odd/even partner. The odd/even partners are pairs of 1-2, 3-4, 5-6, and 7-8. This allows the NetGuardian to view communication traffic in either direction when inserted in the serial communication path between two devices. This is accomplished by going "in" to the NetGuardian with one device and "out" to the other device from the odd/even partner port. Data is passed directly from one port to its odd/even partner without being altered in any way. This ability greatly simplifies troubleshooting communication problems by isolating the non-communicating device. When CHAN is selected, the NetGuardian automatically activates the odd/even partner as CHAN.*
CRFT	Causes the data port to have the same functionality as the front panel craft port.
CAP	Allows the user to capture debug information of a serial device. The debug information is stored in the receive queue of the NetGuardian (See section 3.8 - Monitoring Data Port Activity for more information). This is used primarily as a troubleshooting feature.
ECU	For use if an ECU is connected to this port (see section 2.13).

Table 2.D Data port type descriptions.

* Baud rates for the odd/even pairs can be set to any available rate except for any combination of 19200 and 38400 between the two ports.

2.4.6.1 RTCP Data Port

The RTCP, or Raw TCP data port, negates Telnet negotiation and will allow all characters (including [FF]) to pass straight through from IP to serial or serial to IP.

2.4.6.2 HTCP Data Port

An HTCP, or High-speed TCP data port, which operates in Telnet Raw mode, is essentially the same as a RTCP port except that it has better performance and is more robust when transferring streaming data (like a data file). Unlike RTCP ports, the user can only assign 1 port as HTCP.

2.4.6.3 Direct and Indirect Proxy Connections

The NetGuardian supports two proxy connections, direct and indirect. In a direct proxy connection, the user enters an IP address and port number to Telnet directly to a TCP serial port. In an indirect connection, the user navigates the TTY menu to select a proxy port. Since the TTY interface is password protected, indirect connections are preferred. Some users prefer to disable direct proxy for all connections in order to enforce the password security provided by the TTY interface. One way to disable proxy connections is to set the proxy port to an uncommon value. This restricts the access of other users, but it is more convenient and secure to set the data ports to "off" in the Type field. When set to off, the port is no longer associated with a TCP socket, which effectively disables the port from direct access.

Use the following steps to select proxy connections:

1. From the Edit > Ports screen, scroll down to the Data Ports section.
2. Enter a description and click on the TCP link—see Figure 2.6.
3. Under the Type column click on the drop-down menu and select the appropriate proxy connection. Refer to Figure 2.7.
4. Click the Submit button to save your configuration settings.

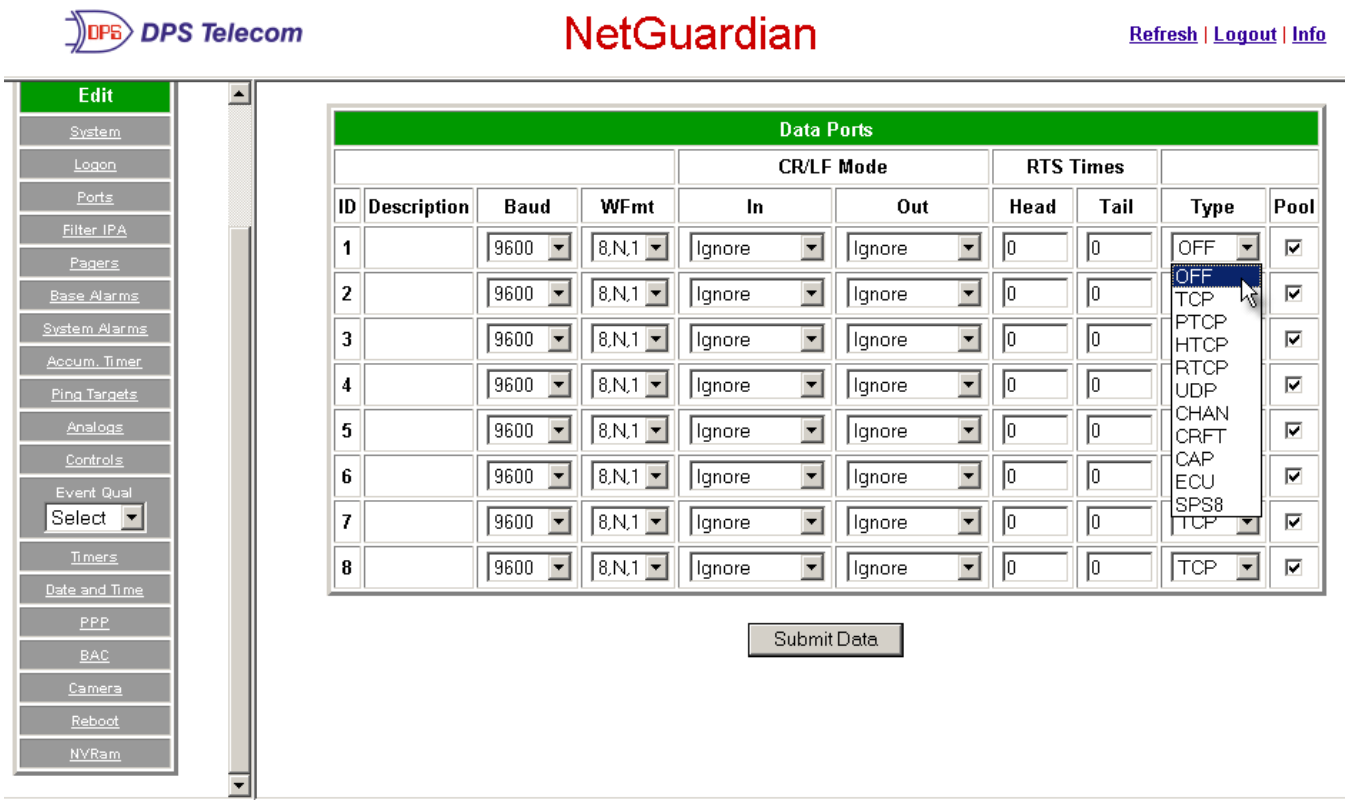


Fig. 12. Setting proxy connections.

2.4.6.4 Defining SPS8 Ports

The SPS8 port type can be selected in the Type option when configuring data ports with NGEdit or the Web Browser interface. You may edit SPS8 port descriptions in NGEdit only. The Web Browser interface will allow the user to set SPS8 type, but not the port descriptions.

The Serial Port Switch 8 (SPS8) is an external device hub that allows the connection of up to eight serial port devices to a single NetGuardian data port. There may be only one SPS8 data port type.

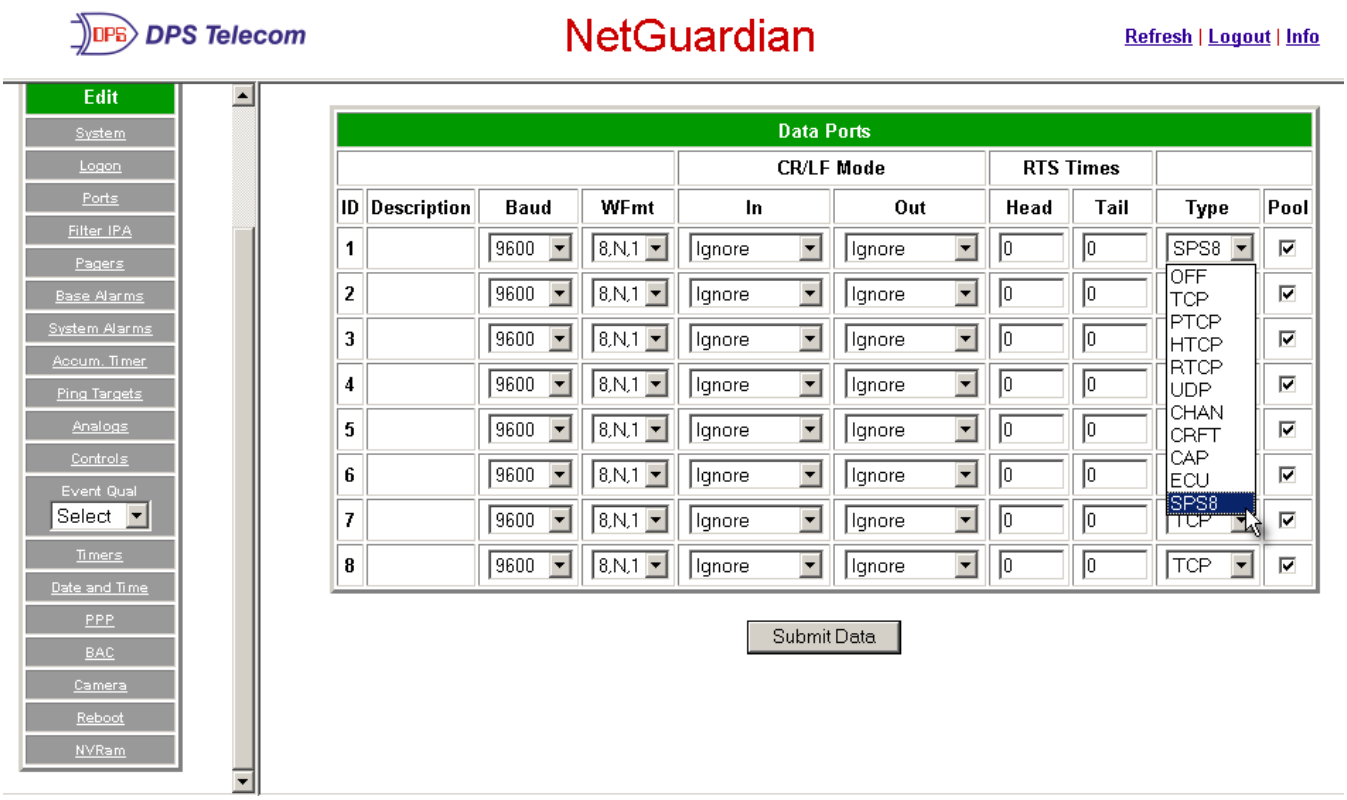


Fig. 2.8 Select SPS8 port type from the Edit > Ports, Data Ports screen.

Use the following steps to select a SPS8 port:

1. From the Edit > Ports screen, scroll to the Data Ports section.
2. Enter a description and click on the TCP link—refer to Figure 2.6.
3. Under the Type column, click on the drop-down menu and select SPS8—see Figure 2.8.
4. Click Submit to save your configuration settings.

Note: If you initialize the NVRAM, the NetGuardian will erase all SPS8 port descriptions.

When an SPS8 port is selected, the NetGuardian will negotiate the connection for the user. To break the SPS8 connection and return to the normal NetGuardian interface, type @@@ and press <Enter>. SPS8 ports do not support direct proxy. You must navigate via the TTY menu. The port should be set to type "TCP" if interfacing an IAM-5 to SPS8 through a NetGuardian.

2.5 Setting Up Notification Methods from Pagers Window

The Edit > Pagers screen lets you configure several alarm notification methods in addition to pagers. Each notification method is defined as a pager type in this screen. To define a pager as the primary or secondary notification of alarm conditions, select the pager in the appropriate alarm point provisioning screens. Refer to Section 2.6, Configuring Base Discrete Alarms, and Section 2.8, Setting System Alarm Notifications, for more information.

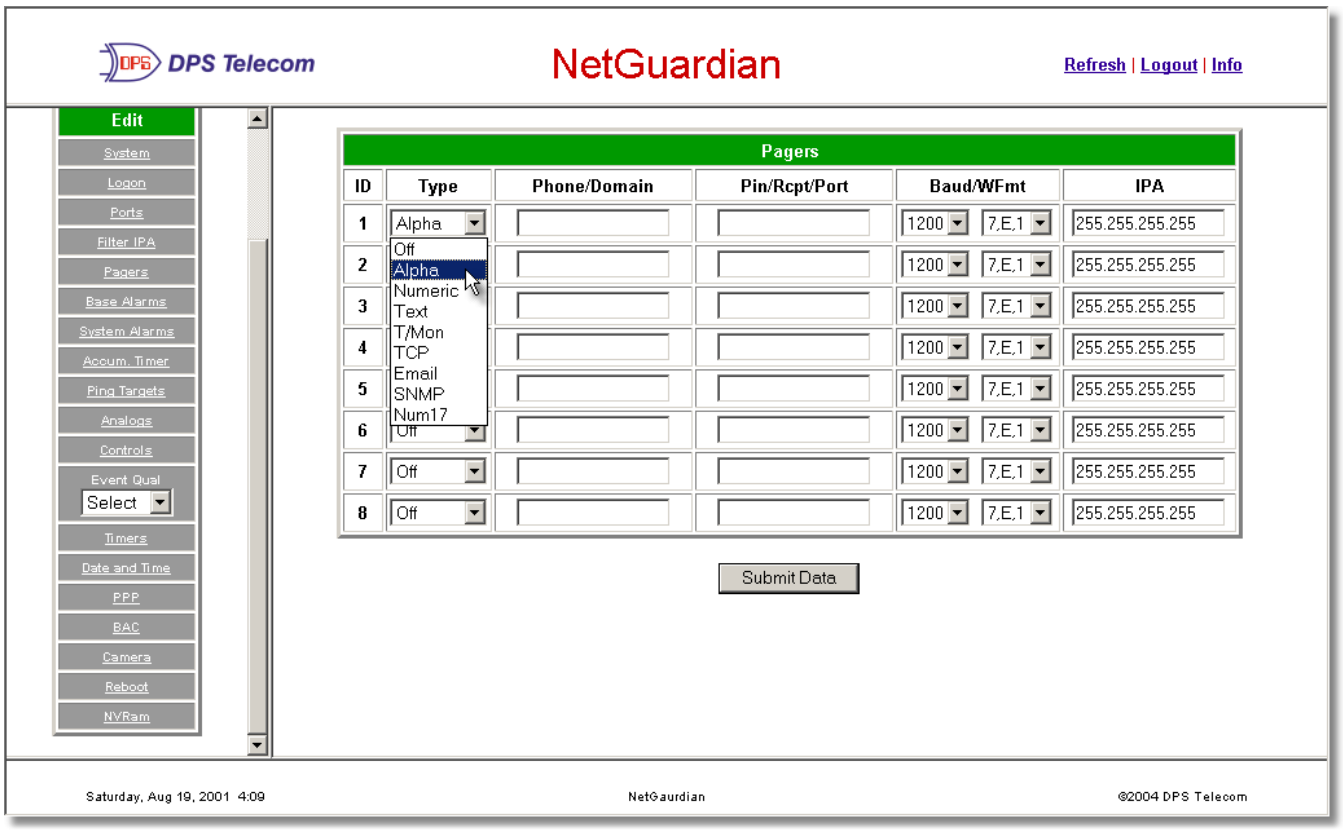


Fig. 2.9 Multiple notification methods are configured from the Pagers screen.

Pager Format	Description
Alphanumeric Paging	Format recognizes numbers, letters, and symbols. Can receive information including alarm point addresses, alarm descriptions, time of alarms, and alarm state.
Numeric Paging	Format recognizes numbers only. Message is reported in the following order: [IP]*[Display] [Address]*[State]. When read on the pager it appears as follows: ########### - #### - #.
Text Paging	Can receive information including alarm point addresses, alarm descriptions, time of alarms, and alarm state. May be accessed using a terminal.
T/MonXM Paging	The IAM may receive alarm information from the NetGuardian via dial-up and display alarm information, alarm description, and threshold status.
Email/SMTP Paging	Provides alarm notification via email, with a description similar to the Alphanumeric pager.
SNMP Paging	May view alarm status from multiple SNMP managers, including the SNMP that alarms are reporting to.
TCP (Telnet) Paging	Alarm status notification via multiple TCP or HTCP ports. Connection from a higher level master must be established for alarm notification.
Num17 Paging	Provides alarm notification in a manner similar to that of the Numeric pager. However, Num17 eliminates the (*) symbol from the page. Message is reported in the following order: [IP][Display][Address][State]. When read on the pager it appears as follows: ################.

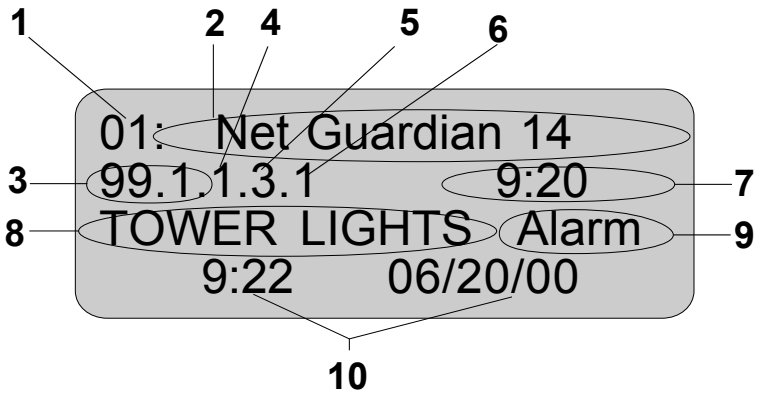
Table 2.E Pager formats.

2.5.1 Alpha Numeric Pager Setup

The alpha numeric pager can receive text messages including alarm descriptions, time of occurrence, and point addresses.

Use the following steps to configure the alpha numeric pager settings:

1. From the Edit > Pagers screen, select an ID number to use. See Figure 2.9 for pager descriptions.
   Note: Pager IDs are used in the alarm provisioning screen to designate the primary and secondary person/device being paged when an alarm condition occurs or clears.
2. Under the Type column, select type Alpha from the drop-down menu—see Figure 2.9.
3. Enter the phone number of the Alpha numeric pager under the "Phone/Domain" heading.
4. Enter a personal identification number under the "PIN/Rcpt/Port" heading.
5. Set the pager data rate (i.e. 300, 1,200, 2,400 or 9,600). The default baud is 1,200.
6. Select a pager word format (Data Bits, Parity, Stop Bits). The default setting is 7,E,1.



1. Number of pages
2. Unit name
3. Port # and Address
   (Applicable to T/Mon and IAM only)
4. Display number
5. Alarm point number
6. Alarm status: 1=alarm, 0=clear
7. Time Net Guardian sent page
8. Alarm point description
9. Alarm status
10. Time & date pager received

Fig. 2.10 Alpha numeric pager description.

2.5.2 Numeric Pager Setup

The numeric pager can receive point addresses of alarms. Use the following steps to configure the numeric pager settings:

1. From the Edit > Pagers screen, select an ID number to use—refer to Figure 2.9.
   Note: Pager IDs are used in the alarm provisioning screen to designate the primary and secondary person/device being paged when an alarm condition occurs or clears.
2. Under the Type column, select Numeric from the drop-down menu—see Figure 2.9.
3. Enter the phone number of the numeric pager under the "Phone/Domain" heading, followed by 7 commas (e.g. "555-1212,,,,,,,"). Placing a comma after the phone number initiates a 2 second pause (per comma). This allows enough time for the pager to answer before the NetGuardian sends the alarm information.
   Note: The Baud/Wfmt and IPA fields are not used from numeric pager types.

2.5.3 Text Paging Setup

Text pages can receive information including the point addresses of alarms, the alarm description, time of the alarm, and state (alarm or clear). The text pages may be viewed using a terminal such as HyperTerminal.

Use the following steps to configure the text paging settings:

1. From the Edit > Pagers screen, select an ID number to use—refer to Figure 2.9.
   Note: Pager IDs are used in the alarm provisioning screen to designate the primary and secondary person/device being paged when an alarm condition occurs or clears.
2. Under the Type column, select Text from the drop-down menu—see Figure 2.9.
3. Enter the phone number of the text paging device under the "Phone/Domain" heading.
4. Set the pager data rate (i.e. 300, 1,200, 2,400 or 9,600). The default baud is 1,200.
5. Select a pager word format (i.e. Data bits: 7 or 8, Parity: none (N), even (E) or odd (O), and Stop Bits: 1). The default setting is 7,E,1.

Note: To set up text paging from T/MonXM see the T/MonXM user manual.

2.5.4 Email Notification Setup

The email pager provides alarm notification via email, with a description similar to that of the alpha-numeric pager. Use the following steps to configure the email notification settings:

1. From the Edit > Pagers screen, select an ID number to use—refer to Figure 2.9.
   Note: Pager IDs are used in the alarm provisioning screen to designate the primary and secondary person/device being paged when an alarm condition occurs or clears.

2. Under the Type column, select Email from the drop-down menu—see Figure 2.9.

3. Enter the domain name of the Email address under the "Phone/Domain" heading. This is the portion of an email address after the "@" symbol in name@domain.com. **Note:** There cannot be any spaces in the domain name.

4. Enter the Email recipient's user name under the "PIN/Rcpt/Port" heading. This is the portion of an Email address before the "@" symbol in the name@domain.com. **Note:** There cannot be any spaces in the recipient's user name)

5. Enter the IP address of the SMTP mail server in the IPA field.

6. Exit the Pagers window by selecting the System window (See Section 2.2). Here you will set up the "from" address sent in Email messages sent from the NetGuardian. The "from" address is formatted using the "name" and "location" fields from the System screen as follows: name@location. Most Email programs can be set to perform a certain action if a message is received from a specified address, such as moving the message to a special "alarms" folder. Use the address entered here for such purposes.

7. Under the "Name" heading, enter a descriptive name to identify the NetGuardian in email messages. (There cannot be any spaces in the designated name)

8. Under the "Location:" heading, enter the domain of the NetGuardian. (There cannot be any spaces in the location name)

Note: The "from" email address is for identification purposes. It is not necessarily a real email address that can be replied to unless one is entered.

2.5.4.1 SMTP POP3 Authentication Support

The NetGuardian also supports SMTP POP3 Authentication.

Unauthenticated E-mails:
The configuration setup will not change. If you want the email to send to user@yourdomain.com, use the following steps:
1. In the Phone/Domain field type "yourdomain.com"
2. In the Pin/Rcpt field type "user". **Note:** The from location is specified by the system info name and location strings, which also do not change.

The "from" location is specified by the system info name and location strings, which also did not change. Use the following steps to configure the "from" location from@fromdomain.com:
1. In the System Info Name field, type "from."
2. In the system info location field type "fromdomain.com."

Authenticated Emails:
If you want to send an authenticated email to "user@yourdomain.com" from "from@fromdomain.com," password="authentic," then use the following steps:
1. In the Pin/Rcpt field type "authentic"
2. In the System Info Name field type "user"
3. In the System Info Location field type "yourdomain.com."

2.5.5 SNMP Paging Setup

The SNMP paging feature allows you to view alarm status from multiple SNMP Managers in addition to the main one, which is setup from the Ethernet Ports menu, that all alarms are reported to.

Use the following steps to configure the SNMP paging settings:

1. From the Edit > Pagers screen, select an ID number to use—refer to Figure 2.9.
   Note: Pager IDs are used in the alarm provisioning screen to designate the primary and secondary person/device being paged when an alarm condition occurs or clears.
2. Under the Type column, select SNMP from the drop-down menu—see Figure 2.9.
3. Set the SNMP port under the "PIN/Rcpt/Port" heading, usually 162.
4. Enter the IP address of the SNMP manager in the IPA field.

2.5.6 TCP Paging Setup

The NetGuardian offers alarm status notification via multiple TCP ports. When an alarm condition occurs, an alarm condition formatted according to Figure 2.11 will be sent to the specified TCP points for use by a higher level master. This connection must be established by the master. Any applicable alarm activity occurring prior to an established connection will be discarded.

Use the following steps to configure the TCP paging settings:

1. From the Edit > Pagers screen, select an ID number to use—refer to Figure 2.9.
   Note: Pager IDs are used in the alarm provisioning screen to designate the primary and secondary person/device being paged when an alarm condition occurs or clears.
2. Under the Type column, select TCP from the drop-down menu—see Figure 2.9.
3. Set the Pin/Rcpt/Port field to the NetGuardian TCP port number where alarm messages will be sent (from 1 to 65,536). Multiple ports can be defined by defining multiple pager IDs as TCP pagers and then entering the desired ports.
4. The TCP message can be viewed via a Telnet session by connecting to the NetGuardian's IP address and the TCP port selected here (e.g. "Telnet 126.10.220.199 5000" if port 5000 is selected and 126.10.220.199 is the unit's IP address. See Figure 2.11 for an example message and Table 2.F for TCP message format information.

<MSG_BEG 00001>
VID : DPS Telecom
FID : NetGuardian SNMP v2.1B.0075
SITE: Yale Office
PNT : 99.01.01.01
DESC: RECTIFIER 1
STAT: CLEAR
DATE: 01/01/2001
TIME: 12:17:02
<MSG_END 00001>

Fig. 2.11 Example TCP message.

Heading	Description
MSG_BEG MSG_END	Sequential message number used to group the message and detect missing messages (e.g. 00001, 00002, etc.).
VID	Vendor ID.
FID	NetGuardian Firmware ID.
SITE	NetGuardian system name.
PNT	Point ID (port.address.display.point) - See Appendix A for display mapping.
DESC	Description set forth in the Alarm parameters.
STAT	Status of the alarm (Clear or Alarm).
DATE	Date the alarm occurred.
TIME	Time the alarm occurred.

Table 2.F TCP alarm message field descriptions.

2.5.7 Num17 Pager Setup

The Num17 pager can receive point addresses of alarms. It is quite similar to the Numeric paging format in the way it receives and reports alarms. However, on certain pager systems the symbol (*) will cause a freeze or other undesirable situation. Num17 eliminates the (*) symbol from the pages it receives and reports alarms as a seventeen-digit series of numbers.

1. From the Edit > Pagers screen, select an ID number to use—refer to Figure 2.9.
   Note: Pager IDs are used in the alarm provisioning screen to designate the primary and secondary person/device being paged when an alarm condition occurs or clears.

2. Under the Type column, select Num17 from the drop-down menu—see Figure 2.9.

3. Enter the phone number of the numeric pager under the Phone heading, followed by commas (for example 555-1212,,,,,,,). Placing a comma after the phone number initiates a 2 second pause per comma. This allows enough time for the pager to answer before the NetGuardian sends the alarm information. The Baud/Wfmt and IPA fields are not used from Num17 pager types.

2.6 Configuring Base Discrete Alarms

All 32 discrete alarms are configured from the Base Alarms window. Description of the alarm point, polarity (normal or reversed), whether to use an SNMP Trap or not, and the primary and secondary pager used to report the alarm, are configured in this window.

Use the following steps to configure base discrete alarm settings:
1. From the Edit menu select "Base Alarms"—see Figure 2.12
2. Enter a description for each discrete input alarm being used.
3. Reverse the polarity by checking the "reverse" box. Normal: contact closure is an alarm. If the Reverse option is selected, the alarm is clear when closed.
4. Select the "Trap" check box to send an SNMP Trap for that alarm point in the event of an alarm condition. Selecting the box = Send Trap, leaving the box blank = Don't Send.
5. Set the Primary and Secondary Pagers with a pager ID from the pager list (See Section 2.5). This allows you to designate pagers. The NetGuardian 832A will notify both the primary and the secondary notification device when point status changes (both alarm and clear).

Note: The pager device can be an ASCII terminal, T/MonXM element manager or IAM element manager, Email, or multiple SNMP managers as well as an alpha or numeric pager.

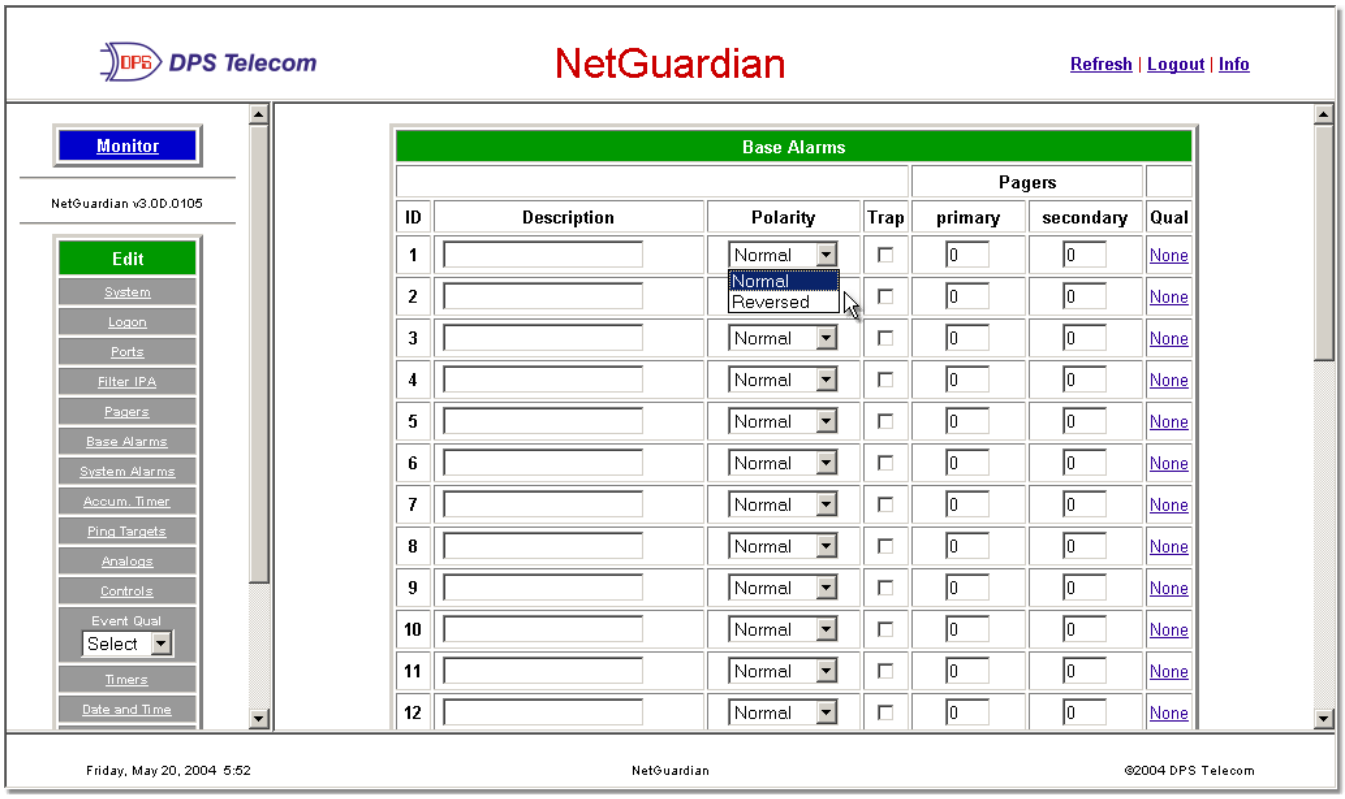


Fig. 2.12 Configure the 32 discrete alarms from the Base Alarms window.

2.7 Event Qualification Timers

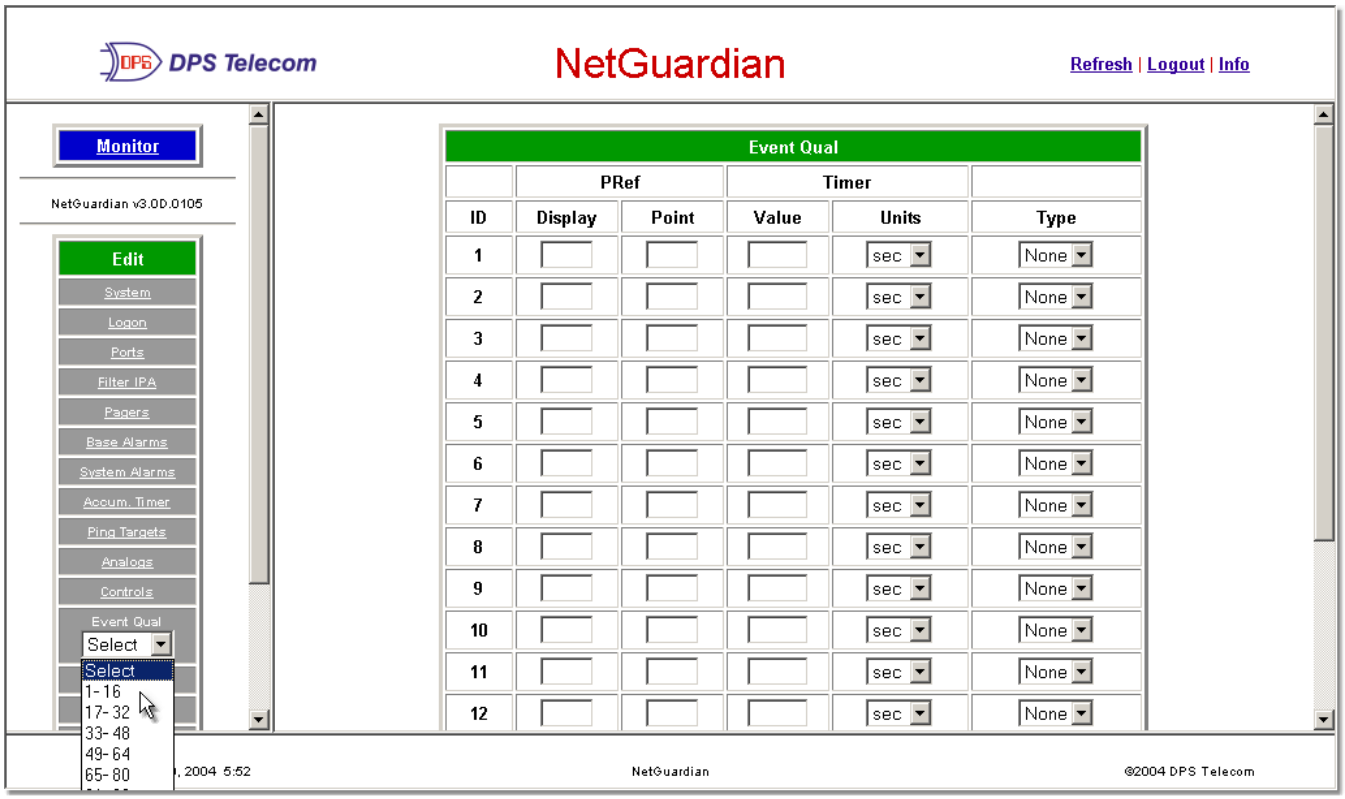


Fig. 2.12 Edit the Even Qualification Timer settings from the Edit > Event Qual screen.

1. From the "Edit" menu in the left hand frame select from the "Event Qual" drop down box.
2. The standard NetGuardian units can have up to 128 Event Quals, grouped in sections of 16.
3. Enter the display and point number for the point you wish to qualify.
4. A list of displays and points can be found in Appendix B, Table B7.
5. Set the value (1 - 127).
6. Set the Units (min, sec, hour).
7. Set the alarm type (Alm, Pri, Sec).
8. To delete the entry, set the "Type" to None.
9. When you are done making changes, scroll to the bottom of the page, and click Submit Data.

2.8 Setting System Alarm Notifications

The system alarms window allows you to individually set the notification method for each system alarm. See Table A2 in Appendix A for housekeeping point descriptions.

1. From the Edit menu, select "System Alarms"See Figure 2.7)
2. Check the "Trap" check box to send an SNMP Trap for that alarm point. Selecting the box = Send Trap, leaving the box blank = Don't Send.
3. Set the Primary and Secondary Pagers with a pager ID from the pager list (See Section 2.5). This allows you to designate pagers. The NetGuardian 832A will notify both the primary and the secondary notification device when point status changes (both alarm and clear).

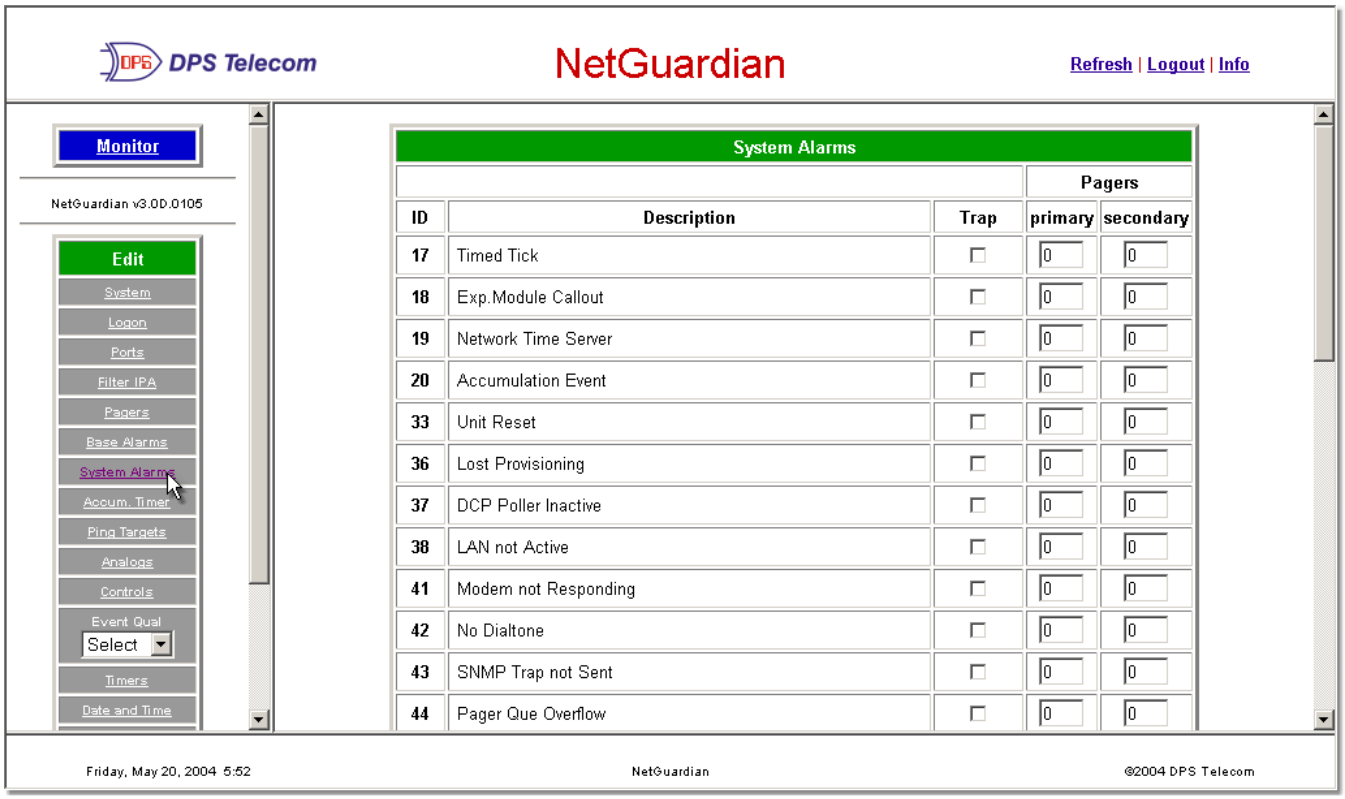


Fig. 2.7 SNMP Traps and primary and secondary pager devices can be selected for each system alarm.

2.9 Configure the Accumulation Timer

The Accumulation Timer keeps a running total of the amount of time a point is in an alarm state to send an "Accumulation Event" system alarm once the total time exceeds a settable threshold. Refer to Table 2.G for field descriptions. To edit your Accumulation Timer settings go to the Edit Menu and select Accum. Timer.

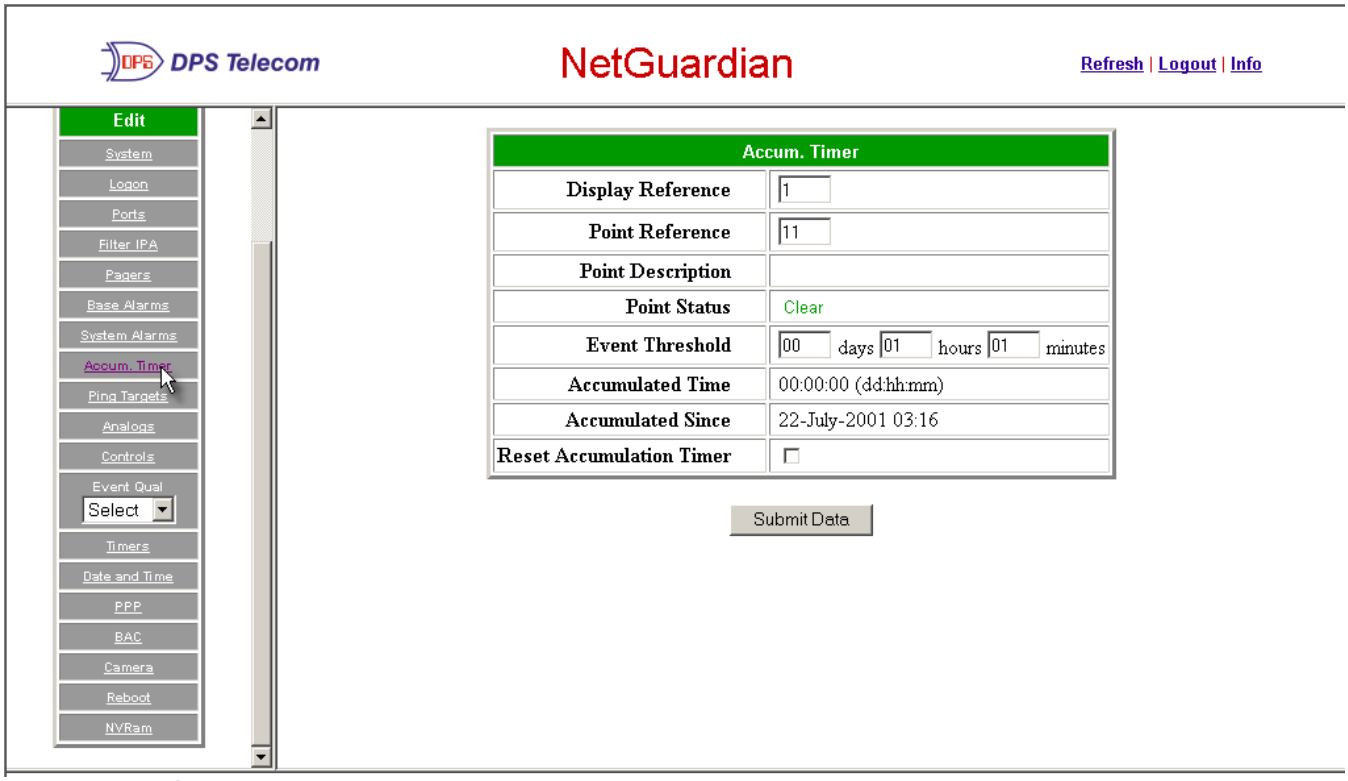


Fig. 2.13 Define the Accumulation Timer settings to send an Accumulation Event alarm.

Field	Description
Display and Point Reference	Indicates which alarm point is to be monitored.
Point Description	The user-defined description of the monitored alarm point.
Point Status	The current status of the monitored point.
Event Threshold	The amount of time allowed to accumulate before the "Accumulation Event" system alarm is set. Maximum is 45 days.
Accumulated Time	The total time the monitored point has been in an ALARM state.
Accumulated Since	Indicates the last time the accumulation timer was reset.
Reset Accumulation Timer	Placing a check mark here will reset the timer when the user presses the Submit button.

Table 2.G Fields in the Accumulation Timer screen.

2.10 Configuring Ping Targets

Each of 32 the ping targets can be provisioned with a description, an IP address, a choice whether to send SNMP Traps, and the primary and secondary pager devices being used.

1. From the Edit menu, select Ping Targets—see Figure 2.14.
2. Enter a description of the device to be pinged.
3. Enter the IP address of the device to be pinged.
4. Set the (SNMP) Trap. Checking the box designates that an SNMP trap will be sent when an alarm condition exists. Leaving the box blank designates that an SNMP trap will not be sent when an alarm condition exists.
5. Select your Primary and Secondary pager devices with a pager ID from the pagers window (See Section 2.5). The NetGuardian 832A will notify both the primary and the secondary notification device when point status changes (both alarm and clear).

Note: See Section 2.11 for timing information.

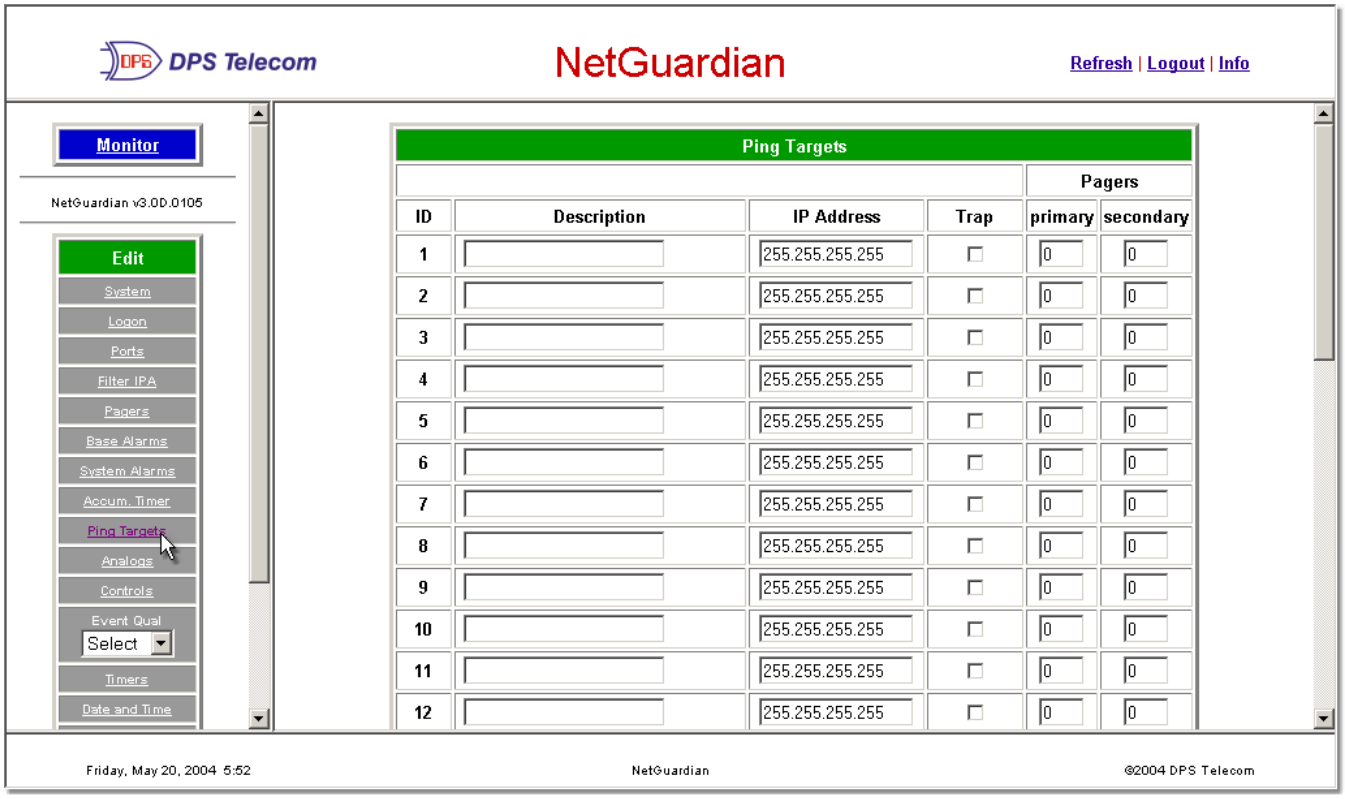


Fig. 2.14 Configure the ping target parameters from the Ping Info screen.

2.11 Analog Parameters

Each of the NetGuardian 832A's analog channels must be individually configured to monitor data. The ADCs (analog to digital converters) support a range of -70 to +94 VDC. There are four alarm trip points (thresholds) in ascending order: major under, minor under, minor over, and major over. You can choose the values for each of the thresholds on all channels. As with the other alarms, you can designate whether or not to send an SNMP Trap when a threshold is crossed. The primary/secondary pager used to report the alarm is also set here. The thresholds must be set from Under to Over in either ascending or descending potential (or current) order. Thus the settings of -10, -5, 5 and 10 corresponding respectively to major under, minor under, minor over and major over is valid.

The analog alarms are set to measure voltage by default and the thresholds are reported as "native units". For example, Channel 3 below is measuring outside temperature. If you were using a sensor with a measurable temperature range between -4 degrees to +167 degrees Fahrenheit (-20 degrees to +75 degrees Celsius). The

voltage for that channel varies between 1 and 5 VDC for that sensor, which is to be reported as degrees Fahrenheit ("native units") where 1 volt represents -4 degrees Fahrenheit and 5 volts represents +167 degrees Fahrenheit. (See Figure 2.9b)

To change any one analog alarm to measure current instead, a circuit board jumper setting must be changed. Refer to the PCB settings section of the NetGuardian user manual for details on jumper locations and positions. The jumper inserts a 250 ohm shunt resistor across the input to convert the sensors current output to volts. Use ohms law to find the voltage drop across the 250 ohm shunt resistor (multiply the current by the resistance 250 ohms). Please refer to the operation manual for your sensor to determine any other conversion factors. This will allow you to correctly set the thresholds for over and under conditions.

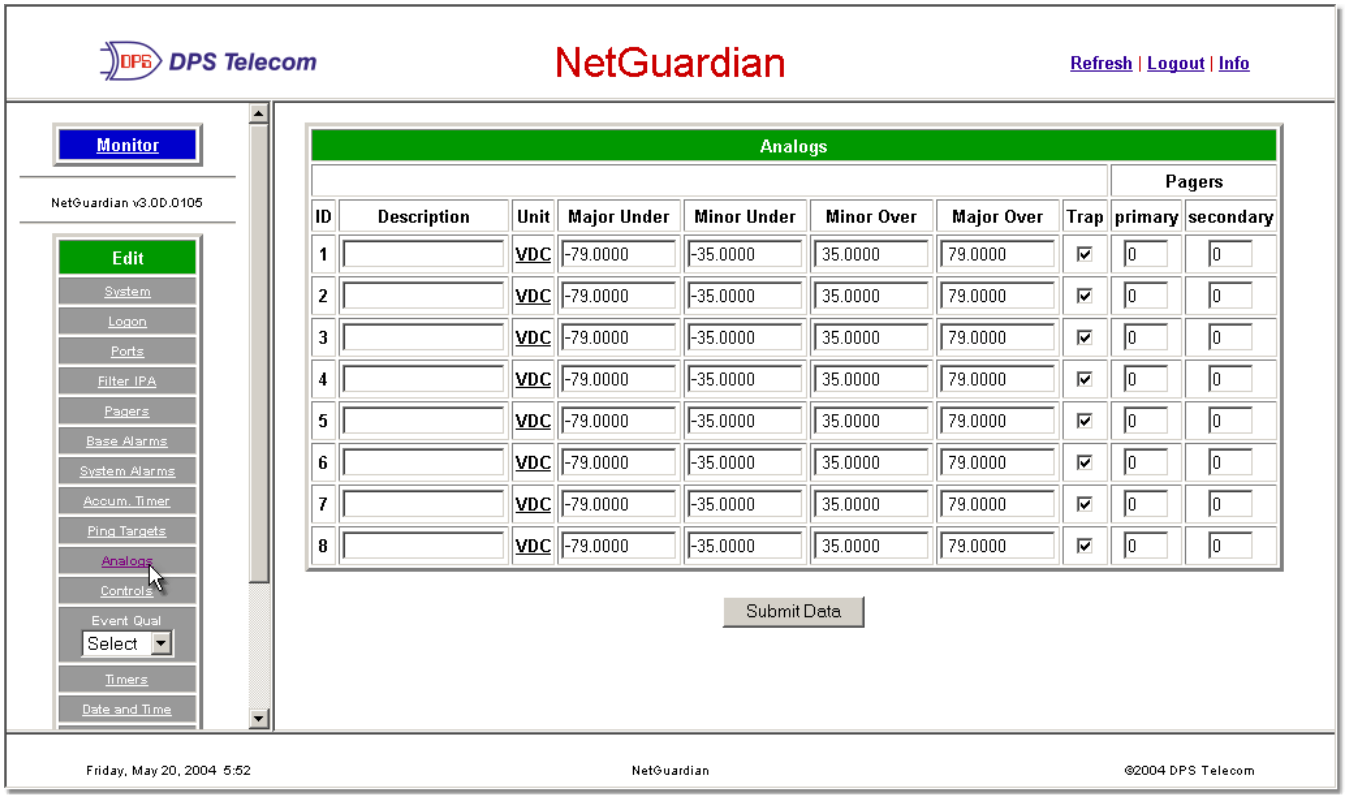


Fig. 2.15 The Analog Parameters can be viewed and changed from the Analogs screen.

1. From the Edit menu, select Analogs.
2. Enter a description for each analog channel being utilized.
3. Click on the "Unit" abbreviation (i.e. VDC, RH, F, etc.) to set the reference units and the native units for that Analog Channel—see Figure 2.16.
4. Set reference 1 (VDC) to the minimum output (in volts DC) of the analog device being configured.
5. In the upper space in reference 1 (the space may already contain the abbreviation VDC), enter an abbreviation for the native units (e.g. RH for relative humidity, F for Fahrenheit, etc.).
6. In the space below the abbreviated native unit setting, enter the native unit that corresponds to the minimum output entered in the previous step.
7. Set reference 2 (VDC) to the maximum output (in volts DC) of the analog device being configured.
8. In the upper space in reference 2 (the space may already contain the abbreviation VDC), set an abbreviation for the native units (i.e. RH for relative humidity, F for Fahrenheit, etc.).
9. In the space below the abbreviated native unit setting, enter the native unit that corresponds to the minimum output entered in the previous step and submit the data.
10. Follow these steps for each Analog Channel being configured.

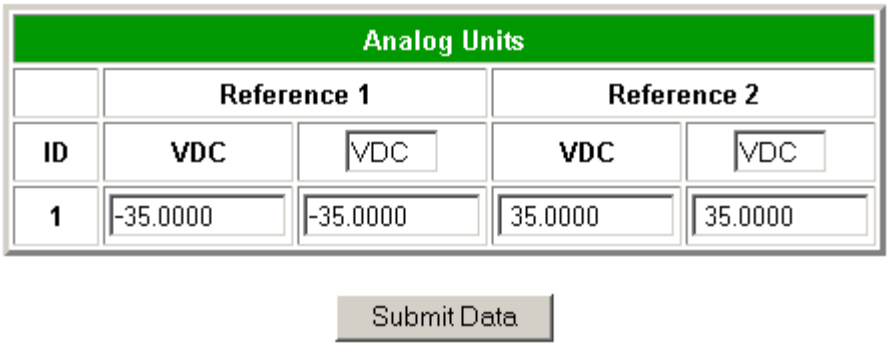


Fig. 2.16 Reference 1 and reference 2 correspond to the minimum and maximum output values of your analog device, respectively.

2.11.1 Integrated Temperature and Battery Sensor (Optional)

The optional integrated temperature and battery sensor allows the user to monitor surrounding temperature as well as the unit's current draw. This is only available if the NetGuardian was purchased with this option. If using the temperature or battery sensor, you must dedicate an analog port to each one (see user manual for connection information).

Temperature Sensor

1. Enter a description in the analog channel you are using for the integrated temperature sensor (either 4 or 8).
2. Click on the unit abbreviation (e.g. VDC) to bring up the analog units screen.
3. In the upper space in reference 1 (the space may already contain the abbreviation VDC) , enter "iF" (internal Fahrenheit) - see Figure 2.9b. This enables the NetGuardian's pre-configured temperature settings. Repeat this step for reference 2.
4. Set your desired thresholds (see Section 2.9 for instructions).

Current Sensor

1. Enter a description in the analog channel you are using for the integrated current sensor (either 5 or 7 for power feed "A" or 6 for power input "B").
2. Set your desired thresholds (see Section 2.9 for instructions). Be sure to set your thresholds in reference to your NetGuardian's power input (e.g. -24VDC, -48VDC, or wide range).

2.11.2 Analog Polarity Override

"iF" : internal temperature sensor
"oV+" : override polarity VDC to positive
"oV-" : override polarity VDC to negative

Clients with positive powered NetGuardians may want to use this feature if they are using the internal battery sensor. The Web Browser monitor will override "oV+" and "oV-" tags and show "VDC". That way you will not have to view an uncommon looking tag while in monitor mode.

2.11.3 Analog Step Sizes

Analog Step Sizes	
Input Voltage Range	Resolution (Step Size)
0 — 5 V	.0015 V
5 — 14 V	.0038 V
14 — 30 V	.0081 V
30 — 70 V	.0182 V
70 — 90 V	.0231 V

Table 2.H Analog step sizes.

2.12 Configuring the Controls (Relays)

The Relays of the NetGuardian 832A can be identified and configured using the Controls window. A description can be entered for each of the relays. You can also designate whether or not to send SNMP Traps when a relay is actuated. Relays are normally open (N/O) by default. A circuit board jumper can be changed for each control to make it normally closed (N/C). Refer to the NetGuardian user manual for PCB settings and jumper positions.

1. From the Edit menu, select "Controls"—see Figure 2.17.
2. Enter a Description for each control/relay being used.
3. Set the "Energize State" to either Normal or Inverted. Normal sets the relay's normal electrical state to "De-energized." Inverted sets the relay's normal electrical state to "Energized." (The Energize State is different than the normal state of the physical contact closure position of each relay, which is determined by circuit board jumpers.) This gives you the added benefit of being able to "monitor the wire." In the event of a power failure, the relay would de-energize back to it's normal physical contact closure set by the circuit board jumper for that relay. Check your jumper settings and relay connections before setting to Normal or Inverted. Refer to the NetGuardian manual for jumper settings and relay connection options.
4. Set the Trap check box. This designates whether or not an SNMP Trap will be sent when a control point operates.

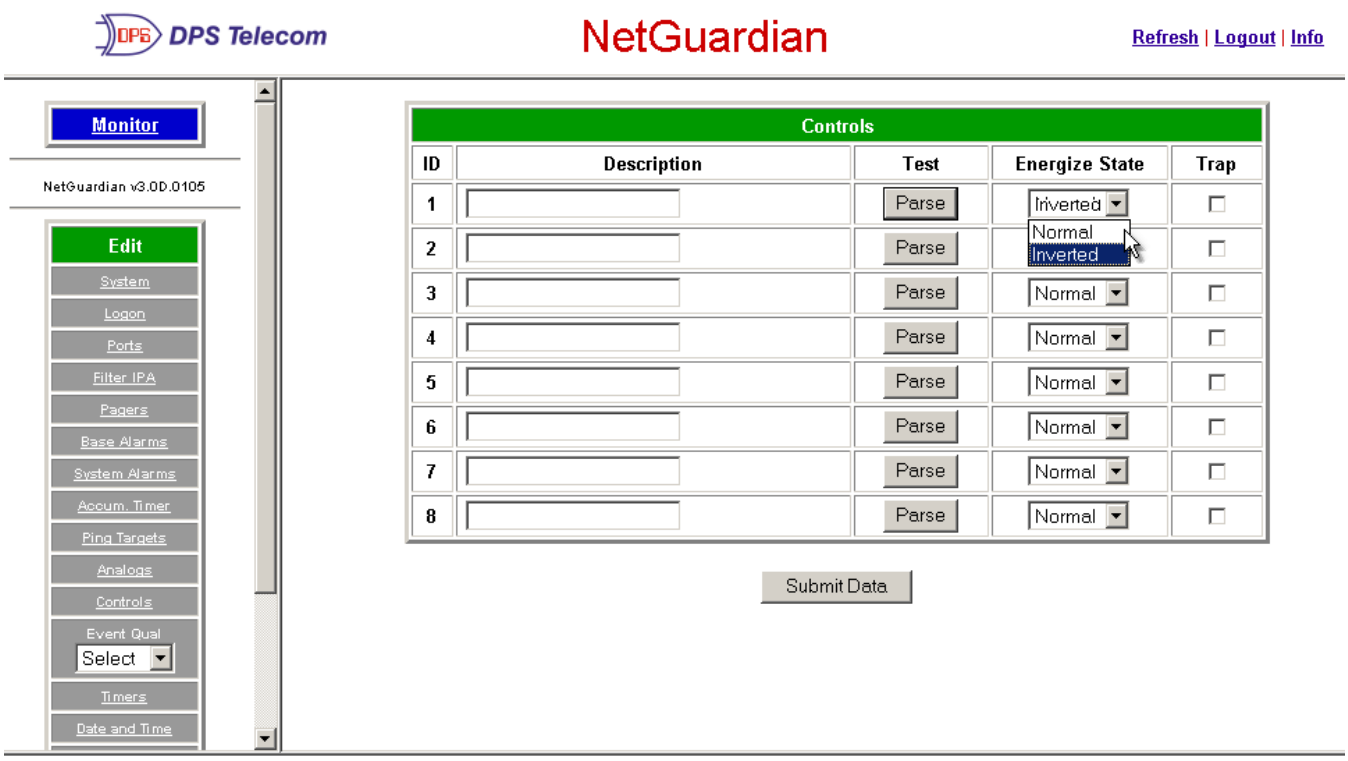


Fig. 2.17 Selecting the Trap field designates that an SNMP trap will be sent when a control point operates.

2.12.1 Activating Relays from an Alarm Point's Change of Status

The NetGuardian allows the user to "Echo" an alarm point state to activate a relay. Any of the NetGuardian's discrete alarms, system alarms, ping alarms, or analog alarms may be Echoed to activate a relay in the event that alarm is triggered. However, a relay set to Echo an alarm point cannot be manually activated. To allow the relay to be manually activated while still maintaining it's "Echoed" status, the relay point must be set to "ORed". See sections 2.10.1.1 and 2.10.1.2 for information regarding Echoing and ORing alarm points to relays.

2.12.1.1 Echoing alarm points to relays

1. In the Relay description field, enter the display, alarm point, a dash "-", and the description of the alarm you wish to echo. For example, if echoing discrete alarm 8, enter 01.08-your alarm description (the display and alarm point are formatted as "DD.PP" where DD=the display number and PP=the point number). See Appendix A for a complete list of display and point numbers.

2.12.1.2 Oring echoed alarm points

1. In the Relay description field, enter the display, alarm point, an under-bar "_", and the description of the alarm you wish to set to ORed. For example, if ORing discrete alarm 8, enter 01.08_your alarm description (the display and alarm point are formatted as "DD.PP" where DD=the display number and PP=the point number). See Appendix A for a complete list of display and point numbers.

2.12.2 Relay Operating Modes

A trap is sent on a relay COS for normal or echoed controls when the "send trap option is selected. A trap is also sent when an oRed relay is manually controlled. A trap will not be sent for an ORed relay latched or released due to an alarm echo.

Each relay can be mapped to one alarm point. Any system, base, or expansion point can be used. Multiple alarm points cannot be mapped to the same control.

The operation of a control is determined by the first six characters of the control description. The format "DD.PP" is used to specify the display and point number of the alarm to be mapped to the control.

2.12.2.1 Echoed Mode

An echoed control reflects the state of the alarm for which it is assigned. The user is blocked from using manual control commands, like "opr" and "rls".
Description format "DD.PP-" where DD = Display #, and PP = Point #.
ex.
"01.08-My Control" : Echoes the state of the alarm at display 1, point 8 to the relay.

2.12.2.2 ORed Mode

An ORed control is active if the alarm for which it is assigned is active or if the control has been manually activated. The user will see the relay mode displayed in red text.
Description format "DD.PP_" where DD = Display #, and PP = Point #.
"01_08_My Control" ORs the state of the alarm at display1, point 8 to the relay.

2.12.2.3 Normal Mode

Relay energized state is similar to alarm point polarity. A normal control is latched when the relay state is "opr", and open when the relay state is "rls". Conversely, an inverted control is latched when the relay state is "rls", and open when the relay state is "opr".
Description does not follow formatting for echoed or ORed modes.
"My Control", Normal relay operation.

2.12.3 Override Default Relay Momentary Time Using Event Qualification

1. Select an event qual group from the edit menu.
2. In the display text box, type 11.
3. In the point text box, type the number of the relay you would like to change.
4. In the value box, type the amount of time. You may not select more than 127 units.
5. In the Units box, select seconds, minutes, hours.
6. In the Type box, select Alm.

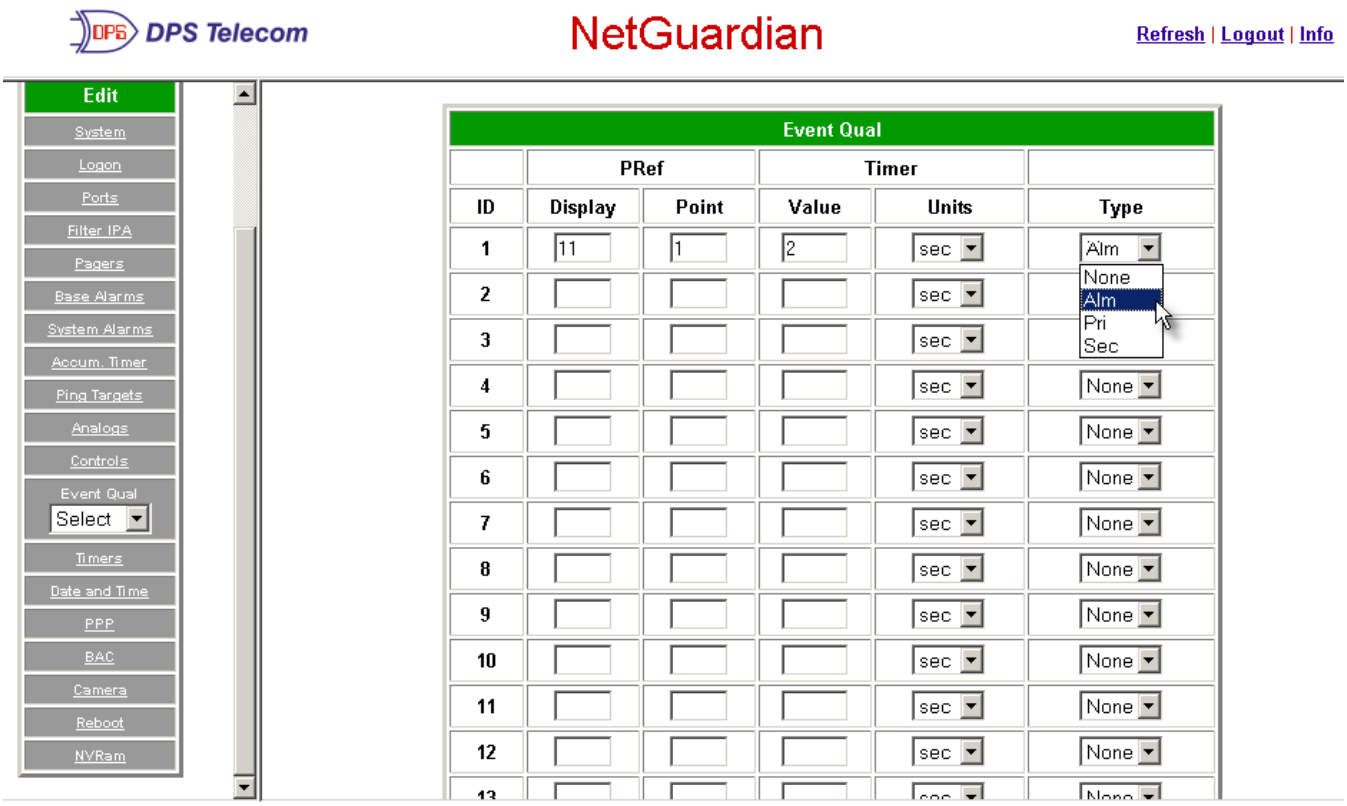


Fig. 2.18 Using Event Qualification.

2.12.4 Derived Control Relays

"_OR" : Set the current operation to OR.
"_AN" : Set the current operation to AND.
"_XR" : Set the current operation to XOR.
"D" : Tag to change the active display number.
"." : Use like a comma to delimit numbers.
"-" : Use to specify a range of points.
Spaces are for readability only.
Precedence of the operations are always left to right.
All number references can either be 1 or 2 digits.

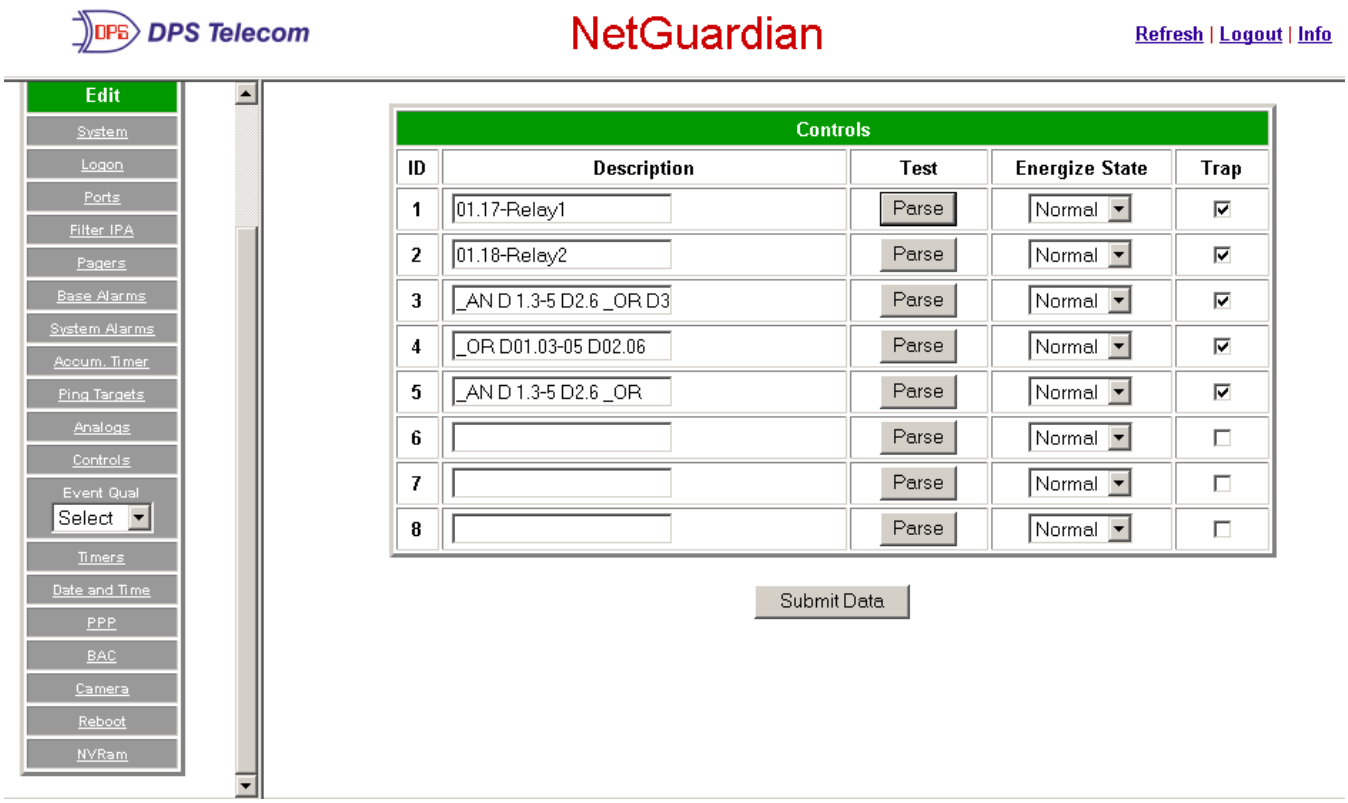


Fig. 2.19 Derived control relays.

"_OR D1.3-5" is logically equivalent to (1.3 || 1.4 || 1.5)

"_AN D 1.3-5 D2.6 _OR D3.7" is logically equivalent to ((1.3 && 1.4 && 1.5 && 2.6) || 3.7)

"_OR D01.03-05 D02.06 _AN D02.07 D03.10.12" is logically equivalent to ((1.3 || 1.4 || 1.5 || 2.6) || (2.7 || 3.10 && 3.12))

"_AN D1.3-5D2.6_OR.7D3.10.12" is logically equivalent to ((1.3 || 1.4 || 1.5 || 2.6) || 2.7 || 3.10 || 3.12))

"CONTROL DESC: _AND1.3-5D2.6_OR.7D3.10.12" will not parse

2.13 Setting System Timers

The system timers allow you to control the rate of your pinging activity, time of speaker sounding, inactivity time for data ports, and discrete alarm detect time. Ping timer settings allow you to balance network traffic against alarm response times. Although you can change the values from their default settings, it is recommended that you use either the default settings or plan your settings so that there is no conflict among the timers. Specifically, the FAIL time should be set to several times the CYCLE time to allow multiple PINGs before a FAIL is declared. Likewise, the CYCLE time should be set to several times the wait time.

Note: The smaller the CYCLE number, the sooner you will find out about failures, however you will increase traffic on your LAN.

1. From the Edit menu, select System Timers—see Figure 2.20.

2. Set the Cycle time. This determines how often the NetGuardian 832A will go through its list of ping targets and attempts to reach them with an ICMP ping. Set the value between zero and 120 and set the units to either

seconds or minutes. Default is 60 seconds.

3. Set the Wait time. The NetGuardian waits after sending a ping request before it determines that the target is unreachable. Set the value between zero and 12 and set the units to either seconds or minutes. Default is 8 seconds.

4. Set the Fail time. This determines the period of time over which, if a unit has not responded, it is considered failed. Set the value between zero and 120 and set the units to either seconds or minutes. Default is 5 minutes.

5. Set the Sound time. This determines how long the NetGuardian's speaker will sound when an alarm occurs or clears. The alarm condition will still be present after the speaker shuts off. The sound timer only affects the duration of the audible alarm annunciation. Set the value between zero and 120 and set the units to either seconds or minutes.

6. Set the Channel time. This determines the period of time over which, if there is no activity on the data ports designated as channel ports (see Section 2.2.4), it is considered failed. Set the value between zero and 120 and set the units to either seconds or minutes. Alarm activity is indicated in Display 11, Point 62—see Appendix A - Display Mapping.

7. Set the Craft time. This determines the period of time over which, if the device connected through a port designated as a "craft" port doesn't reset the timer, an alarm will be triggered. Set between 0 and 120 (min or sec). Alarm activity is indicated in Display 11, Point 63—see Appendix A, Display Mapping.

8. Set the DCP time. Set between 0 and 120 (sec or min). This determines the period of time over which, if the NetGuardian does not receive a DCP poll, to trigger an alarm.

9. Set the timed tick between 0 and 60 minutes. This is a 'keep alive' or 'heartbeat' function that can be used by masters who don't perform integrity checks. For example, if you entered "30", the NetGuardian would notify you every 30 minutes. See System Alarms for paging information.

10. Set the PPP time. Set between 0 and 120.

11. Set the NTP Sync. Set between 0 and 120 (sec or min).

12. Set the Proxy time between 0 and 120 minutes. The proxy timer enables the user to specify how long the NetGuardian should wait during a silent period before timing out and disconnecting a proxy connection. Traffic in either direction will automatically keep the proxy connection alive by resetting the timer for another period.

Note: A proxy timer value of 0 means never time out proxy connections. The default proxy timer value is 20 minutes. Previous NetGuardian versions use a 20-minute proxy timer value as well. PTCP (Permanent TCP) connections never time out regardless of the proxy timer setting.

Warning: DPS does not recommend setting the timer to 0 because a broken but lingering connection may leave the proxy resource unavailable, requiring the user to either reboot the system or reset the port from the TTY interface.

13. Set the Web Edit Timeout time between 5 and 120 minutes. This determines the period of time a web edit page may be active without any activity. A logon is required if a web edit timeout occurs. The default web edit time is 10 mins.

14. Set the Web Monitor Refresh time between 2 and 120 seconds. This timer enables the user to specify how long the NetGuardian should wait before auto-refreshing a monitor page to the web browser. The default web monitor refresh time is 60 seconds.

Note: The timer settings are accurate to + or - 1 tick. This means that if a timer is set to 1 minute, it may actually respond anywhere from 0 to 2 minutes. Therefore, if your target time is 1 minute - set the timer to 60 seconds instead so that it will respond anywhere from 59-61 seconds.

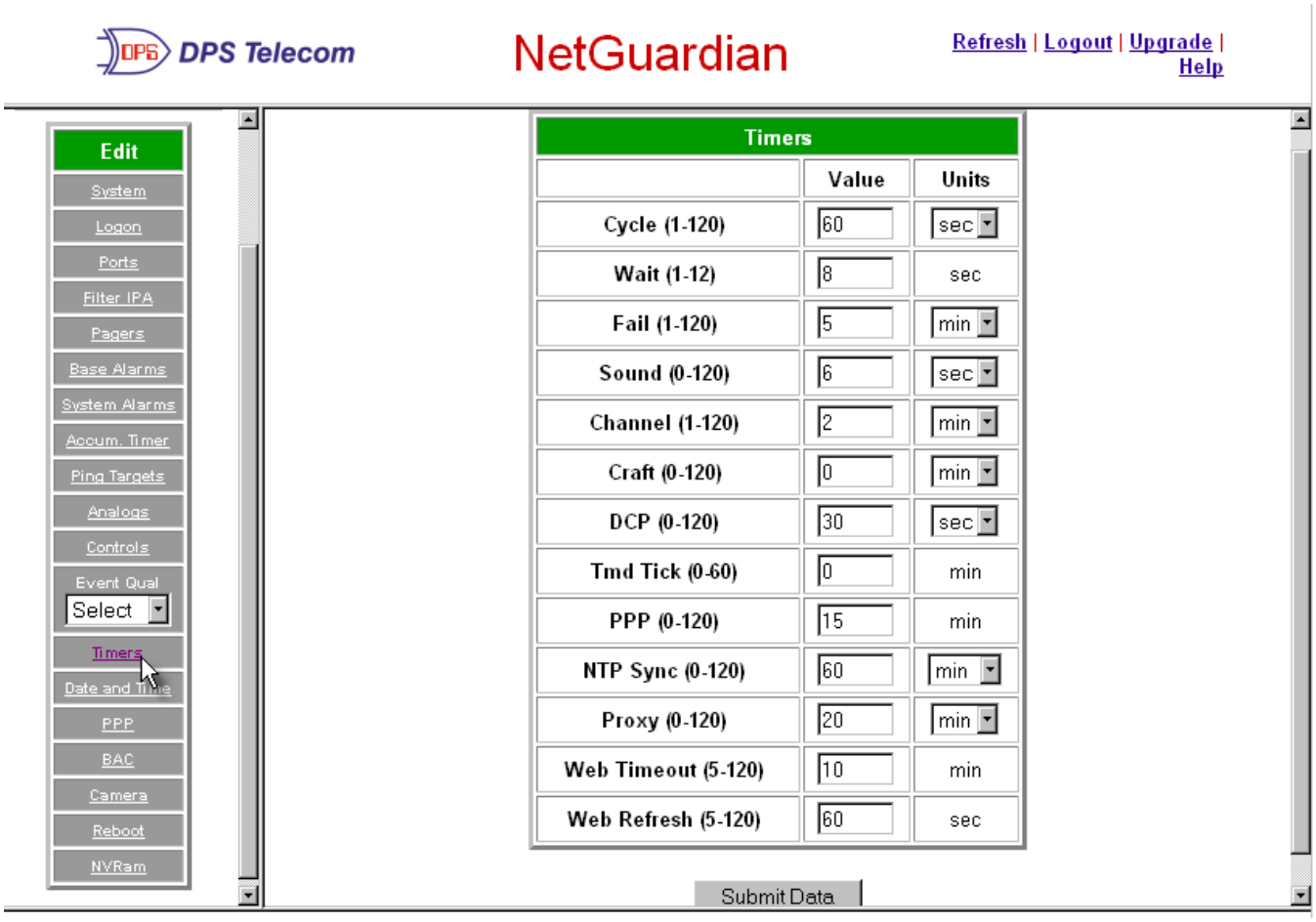


Fig. 2.20 When a target fails to respond to a ping within the fail time period, a fault is declared.

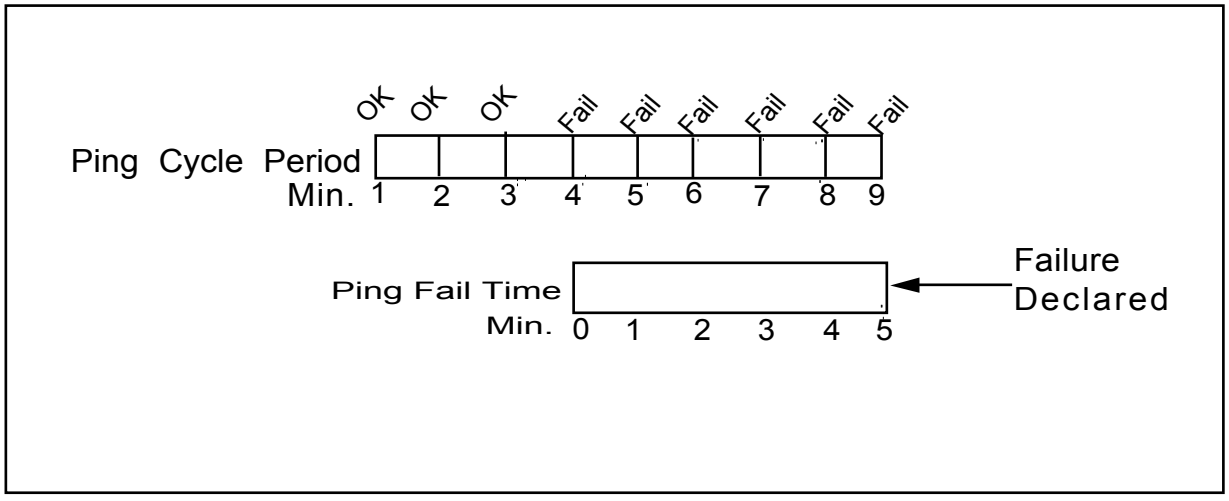


Fig. 2.21 Default timer settings.

2.14 Setting the System Date and Time

The date is entered in the mm/dd/yyyy format and the time is entered in the hh:mm:ss format. The date and time can also be set from an SNMP manager.
1. From the Edit menu, select Date and Time—see Figure 2.22.
2. Enter the date, the day of the week, and time.

Note: The date and time will need resetting following a power failure or reboot unless your NetGuardian is equipped with the real-time clock option.

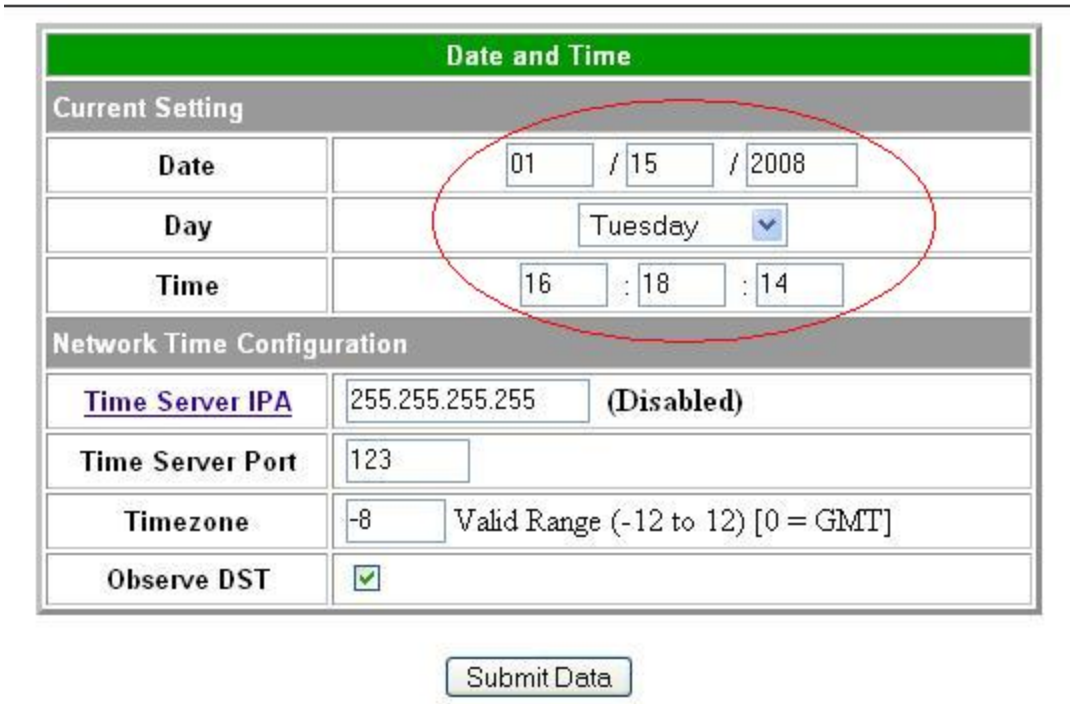


Fig. 2.22 The current date and time can be entered from the Date and Time screen or from an SNMP manager.

2.14.1 Network Time Protocol Support

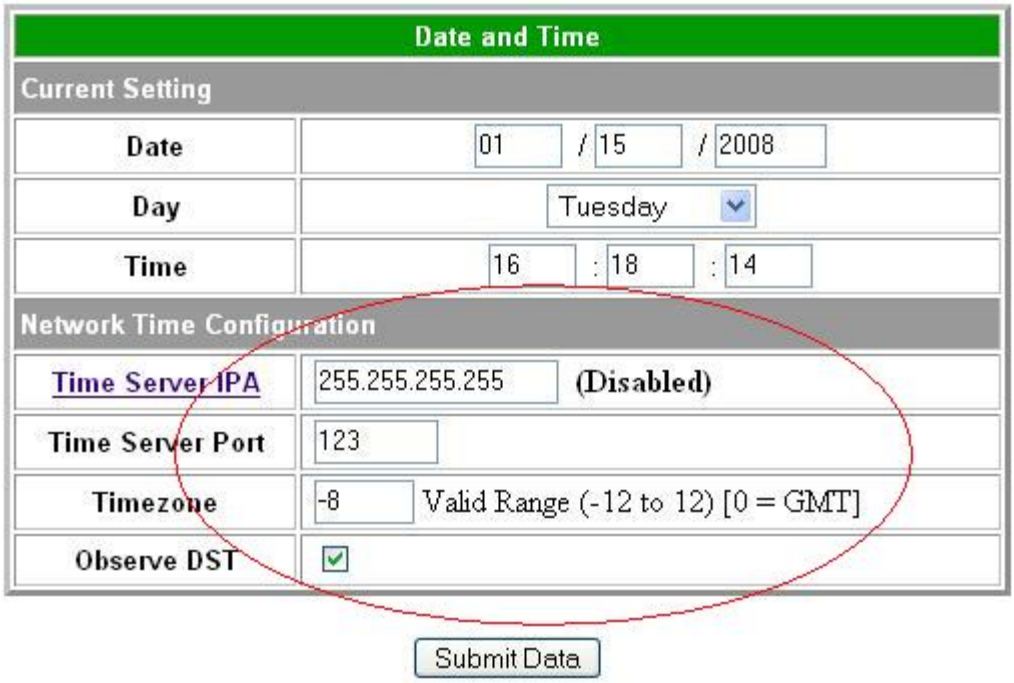


Fig. 2.23 Using the Network Time Protocol.

1. From the Edit Menu, select Date and Time.
2. From the Date and Time edit page, change the "Timezone" to your time zone.
   Note: Here is a link that will help you to find your time zone: http://en.wikipedia.org/wiki/Time_zone
3. Put a check next to Observe DST if you are in an area that observes Daylight Saving.
4. You may also change the server IP Address that the NetGuardian syncs with.
5. If you do not want your net guardian to sync with an NTP server, simply set the Time Server IPA to 255.255.255.255.
6. If Time Server IPA is set to 255.255.255.255, you will be able to manually adjust the date and time.

2.15 Building Access Controller

The Building Access Controller (BAC) option is only available if the BAC is installed on the NetGuardian—see BAC user manual for more information. Enter a password for each door point being used.

The passwords entered here are for turn-up and test procedures only and are only effective until the BAC provisioning information is downloaded from an IAM or T/MonXM master. Once the information is downloaded from T/MonXM, the passwords entered here will be replaced with the new passwords.

Enter the BAC unit ID number. This is the DCP address of the BAC module. It must match the base address being polled by the master. Any range from 1-255 is acceptable or enter zero to disable.

When Direction is enabled, users are required to enter a "1" for "enter" immediately following their password or a "4" for "exit" immediately following their password. Be sure to define the data port you are using for the ECU as an "ECU" type (see Section 2.4.5)

Note: If there is no information downloaded from the IAM or T/MonXM regarding a door point with a NetGuardian password, the NetGuardian password will remain valid.

2.16 Camera Settings

The NetGuardian SiteCam provides users with live streaming video of their remote sites. The direct pan-and-tilt features allows users to visually check the status of their sites from the convenience of their desktop.

1. From the Edit menu, select Camera—see Figure 2.23.
2. Enter the appropriate information in the Camera fields—see Table 2.i for field descriptions.
3. See Section 3.9, Monitoring Camera Activity, for camera viewing options.

Note: In order to have pan-and-tilt controls, your Internet settings must be set to check for newer versions of stored pages at every visit to the page—see Section 2.14.1.

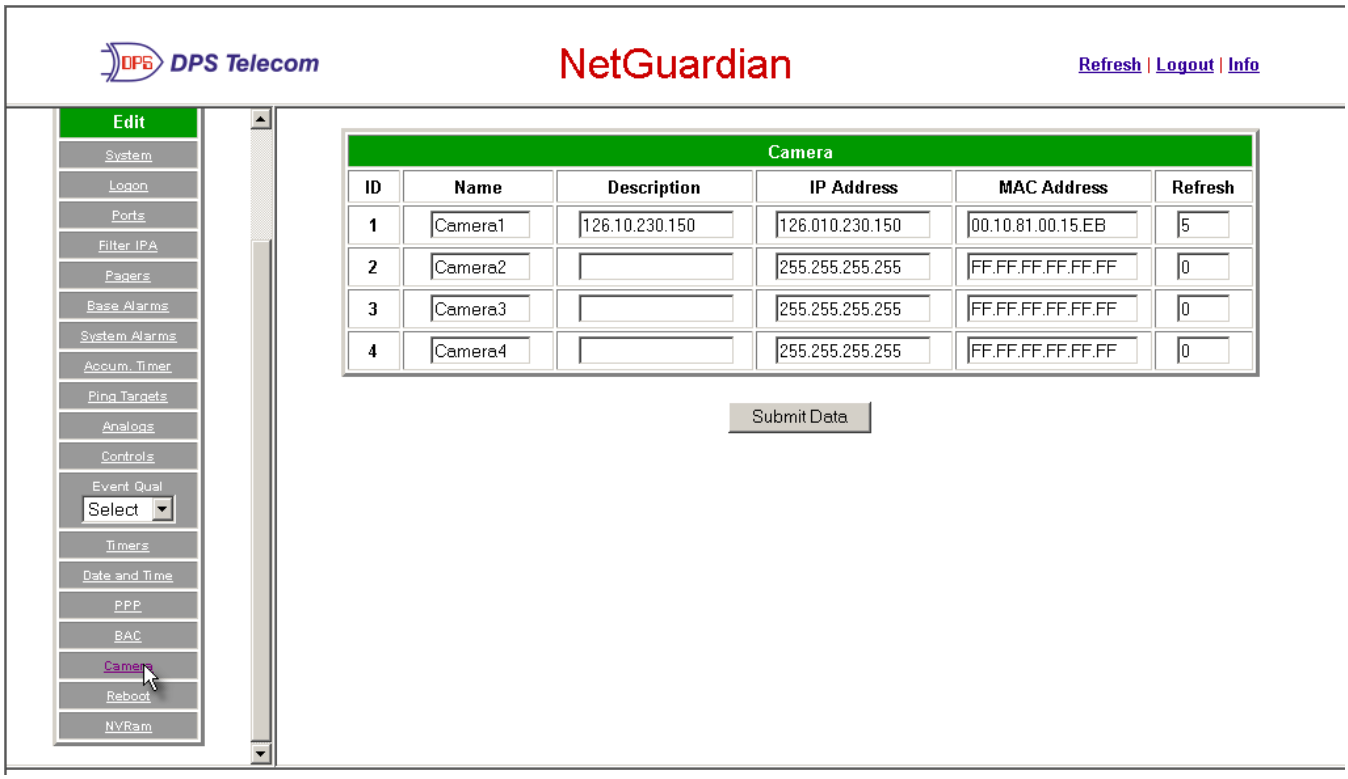


Fig. 2.17 View live streaming video of your remote sites via the NetGuardian's Web Browser.

Camera Field	Description
Name	Enter the name of the camera.
Description	Enter a description of the camera.
IP Address	Enter the IP Address of the camera (not the NetGuardian). The NetGuardian will provision this in the camera. The unit will also send the NetGuardian subnet and gateway information.
MAC Address	Enter the hardware address of the camera (not the NetGuardian).
Refresh	Enter the refresh time. This determines the amount of time (in seconds) that elapses before the image will be updated. Entering 0 will cause uninterrupted, live streaming video (bandwidth rated at 146kB per second).

Table 2.I Camera field descriptions.

Camera Internet Settings

In order to perform the pan-and-tilt functions of the camera, your web browser must be set to check for newer versions of stored pages at every visit to the page. Follow the instructions below.

Note: The directions for checking for newer versions of stored pages may vary depending on what version of Windows you are running. The instructions below are relevant to Windows 2000 only.

1. With the web browser open (Internet Explorer version 5.5 or later), click on "Tools" and select "Internet Options" from the drop-down menu.
2. Click on the "Settings" button under the "Temporary Internet files" heading.
3. Click on the "Every visit to the page" button and click "OK".

2.17 Saving Changes or Resetting Factory Defaults

Your NetGuardian 832A comes equipped with Non Volatile (Nv) RAM which enables the retention of data in the event of power loss. This section of the editor allows you to Write and Initialize the NvRam.
Note: Some changes require a reboot of the NetGuardian to take effect—see Section 2.16.

1. From the Edit menu, select NvRam—see Figure 2.23.
2. Select "Write" to cause the current data in RAM to be written to NvRAM and then verified.
3. Select "Initialize" to reload factory defaults into NvRAM.
   DO NOT SELECT THIS OPTION UNLESS YOU WANT TO RE-ENTER ALL OF YOUR CONFIGURATION INFORMATION AGAIN.
4. Select "Purge BAC" to delete the Building Access Controller profile database.

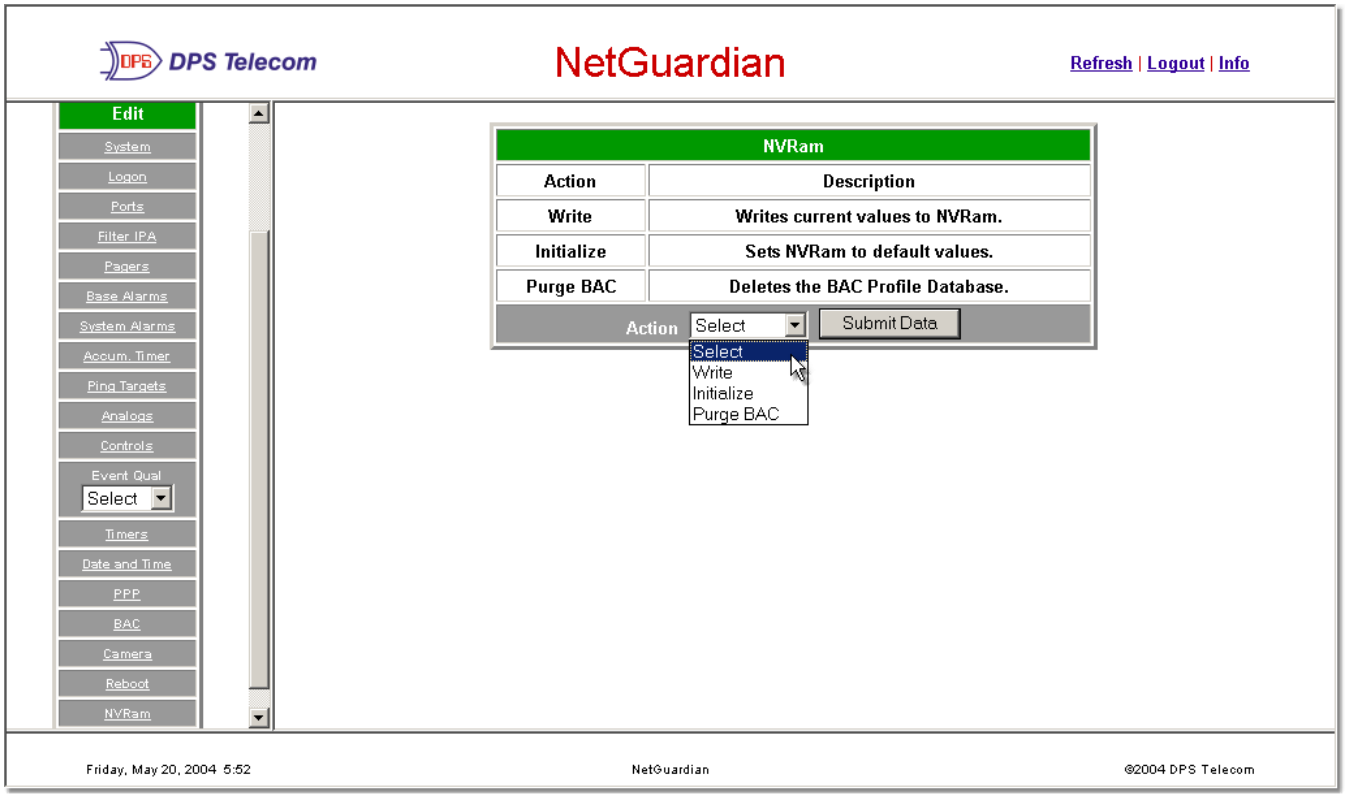


Fig. 2.18 Non Volatile RAM enables the NetGuardian to retain data even through a power loss.

2.18 Rebooting the NetGuardian

Click on the "Reboot" link from the Edit menu to reboot the NetGuardian after writing all changes to NVRAM. Any changes to port settings require a reboot to take effect. The window footer will display the text "Reboot Needed" if a reboot is necessary to initiate changes.

3 Web Server Monitoring Chapter 3

The Web Browser allows you to do full-system monitoring for your NetGuardian 832A which includes all alarms, ping information, relays, analogs and system status.

1. To connect to the NetGuardian from your web browser, you must know it's IP address or domain name if it has been registered with your internal DNS. Enter it in the address bar of your web browser (it may be helpful to bookmark the logon page to simplify access).

2. After connecting to the NetGuardian's IP address, enter your password and click Submit (factory default password is "dpstelecom").

Note: If the edit menu does not appear in the left frame after logging on, it means that another station has already logged on as the primary user.

3.1 Alarm Summary Window

Clicking on the Monitor or Summary buttons shows the Alarm Summary display. The Summary screen gives you a quick indication of any alarms that have been triggered in the NetGuardian's base alarms, ping targets, analogs, system alarms, and any NetGuardian discrete expansions.

Fig. 3.1 The Alarm Summary display can be accessed by selecting either the Monitor or the Summary button.

3.2 Monitoring Base Alarms

This selection provides the status of the system's Base Alarms by indicating if an alarm has been triggered. Under the State column, the word Alarm will appear in red if an alarm has been activated. Clear will be displayed in green when the alarm condition is not present.

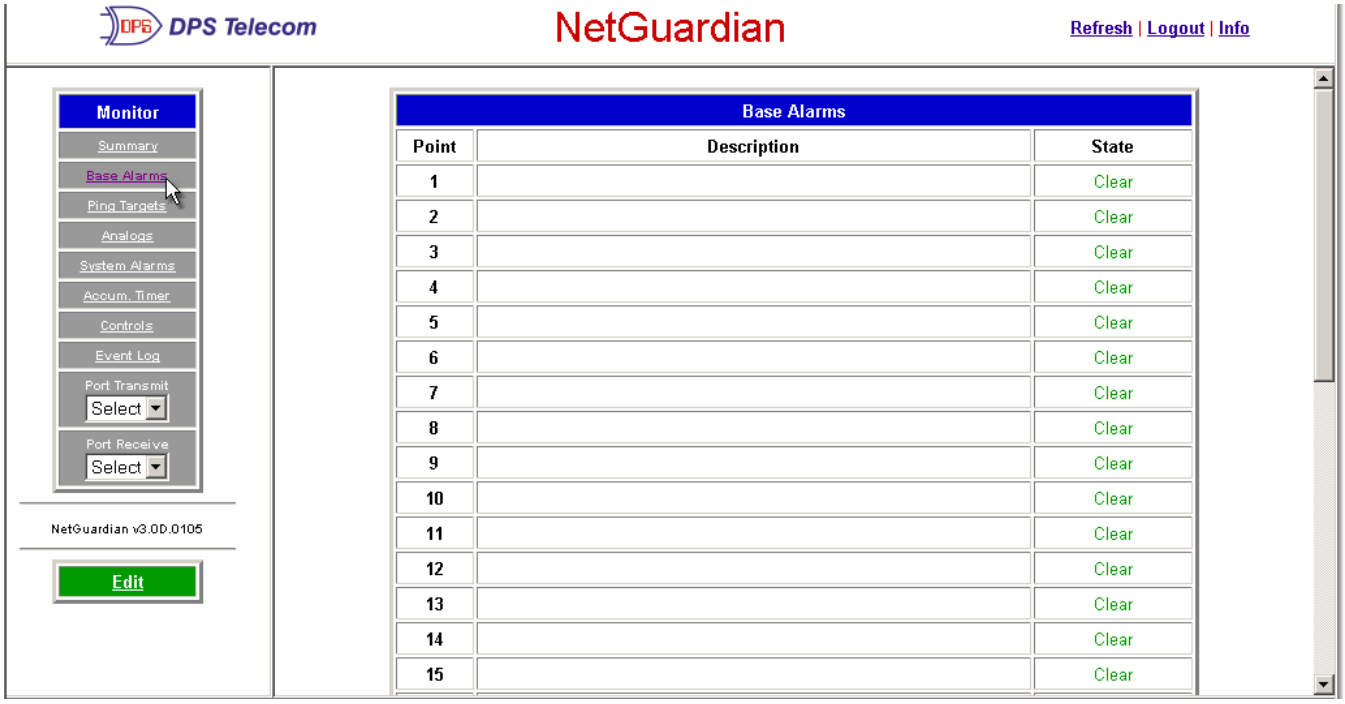


Fig. 3.2 View the status of the Base Alarms from the Monitor-Base Alarms window.

3.3 Monitoring Ping Targets

This selection provides the status of the system's Ping Targets by indicating if an alarm has been triggered. Under the State heading, the word Alarm will appear in red if an alarm has been activated.

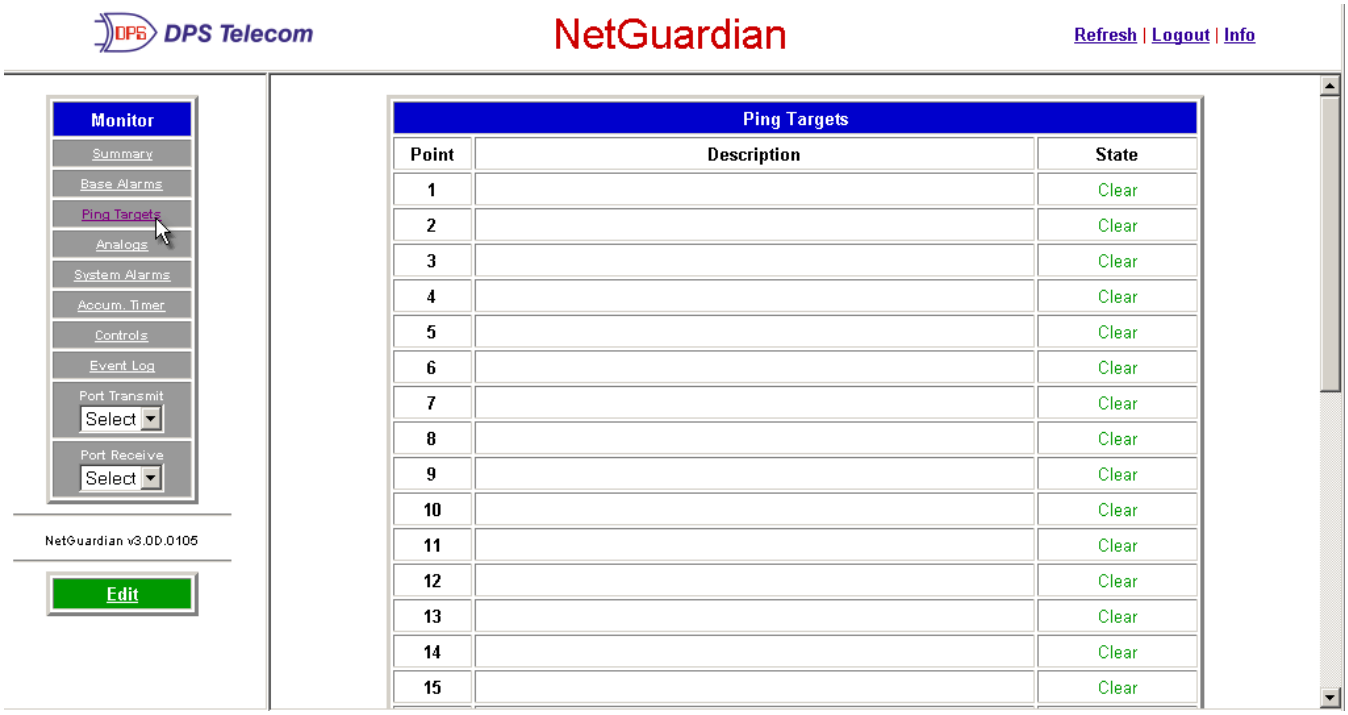


Fig. 3.3 View the status of the Ping Targets from the Monitor > Ping Targets screen.

3.4 Monitoring Analogs

This selection provides the status of the system's Analogs by indicating if an alarm has been triggered. The Analogs window provides a description of each analog channel, the current reading, the units being read, and alarm conditions (major under, minor under, major over, minor over) according to your analog settings.

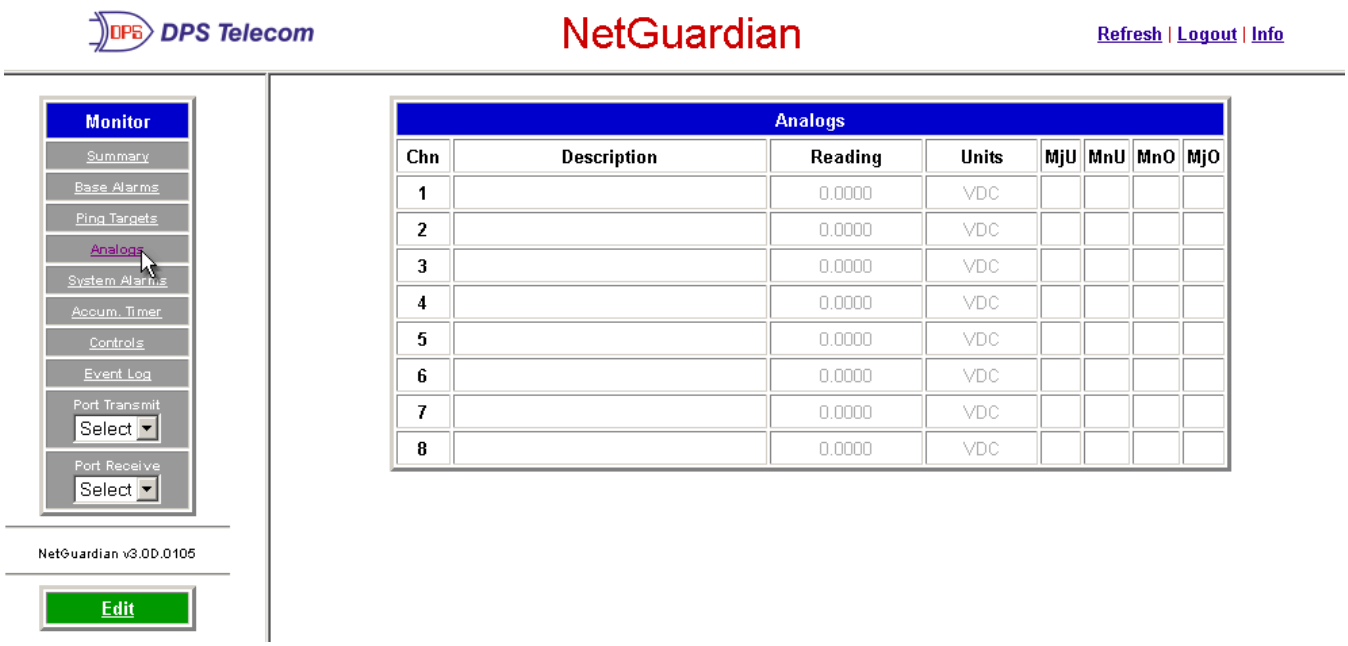


Fig. 3.4 View the status of the Analogs from the Monitor-Analogs window.

3.5 Monitoring System Alarms

This selection provides the status of the System Alarms by indicating if an alarm has been triggered. Under the State heading, the word Alarm will appear in red if an alarm has been activated. Refer to Appendix A for System Alarm Trap numbers.

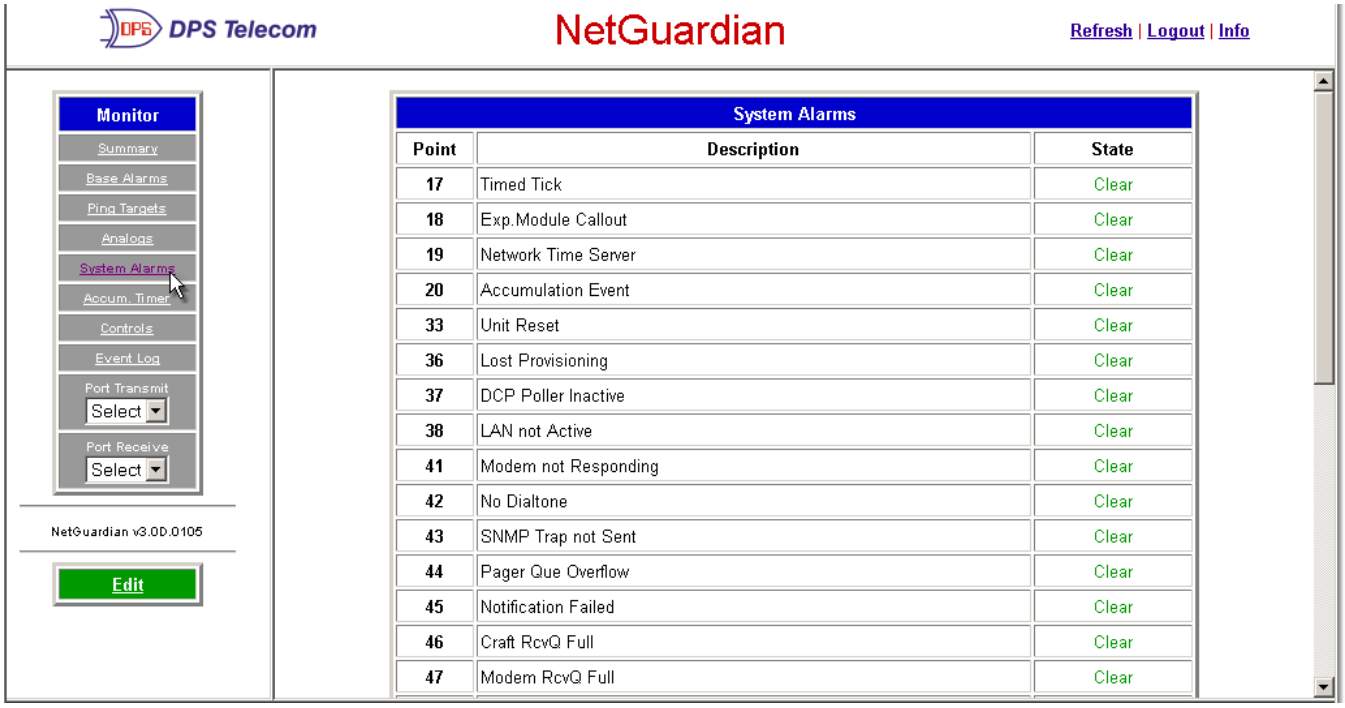


Fig.3.5 View the status of the System Alarms from the Monitor-System Alarms window.

3.6 Operating Controls

1. Select Controls from the Monitor menu.
2. Under the State field, choose a command (Opr - operate, Rls - release, or Mom - momentary).
3. Click on Submit Data to issue the control.

Note: The control relay's normal state - open or closed - is determined by a PCB jumper. Operating a control thus changes the normal state of the relay (energizes it) until it is released (de-energized). The momentary command energizes the relay for approximately one second before it is released again.

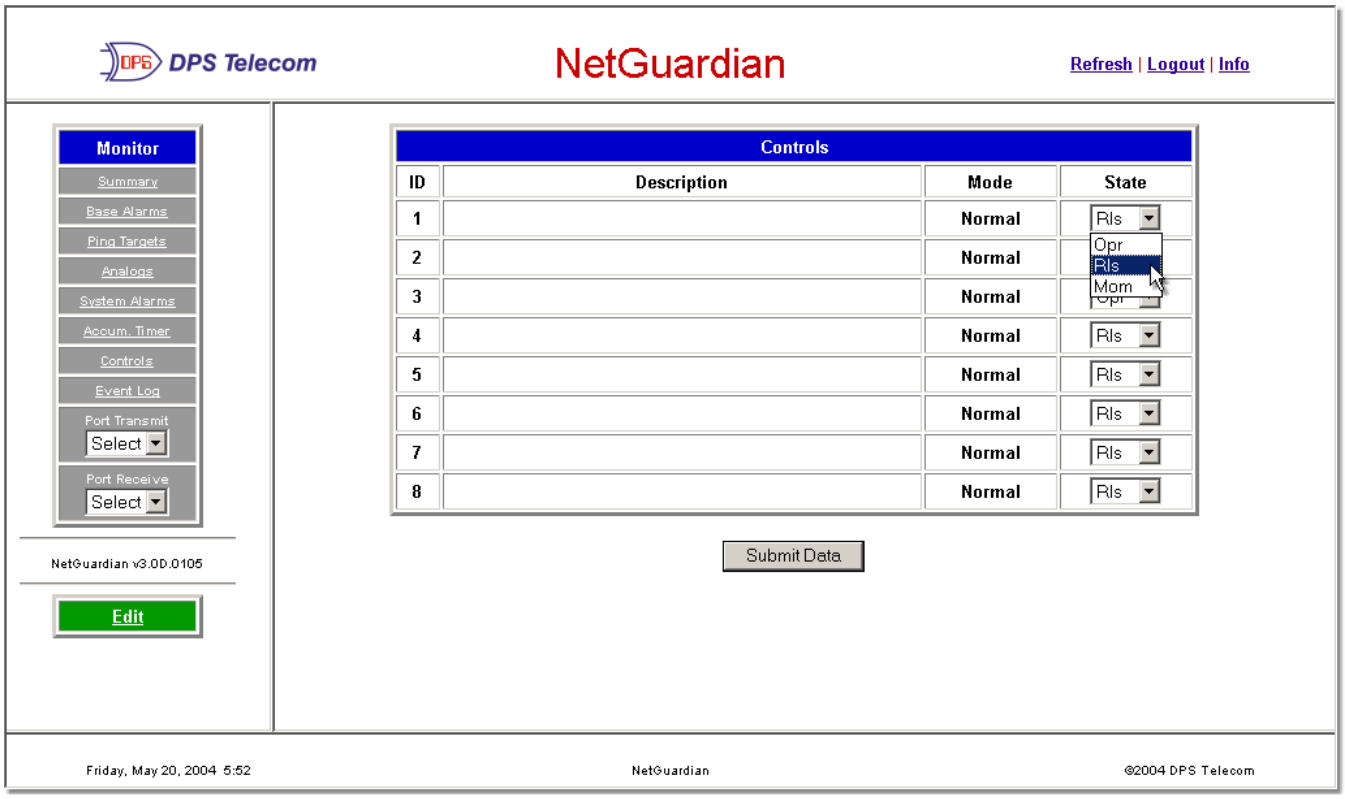


Fig. 3.6 Issue controls from the Monitor > Controls window.

3.7 Event Logging

The event log allows the NetGuardian to post and monitor up to 100 events including power up, base and system alarms, ping alarms, analog alarms, and controls. Posted events for the various alarms include both alarm and clear status. See Table 3.A for Event Alarm field descriptions.

Note: All information in the Event Log will be erased upon reboot or a power failure.

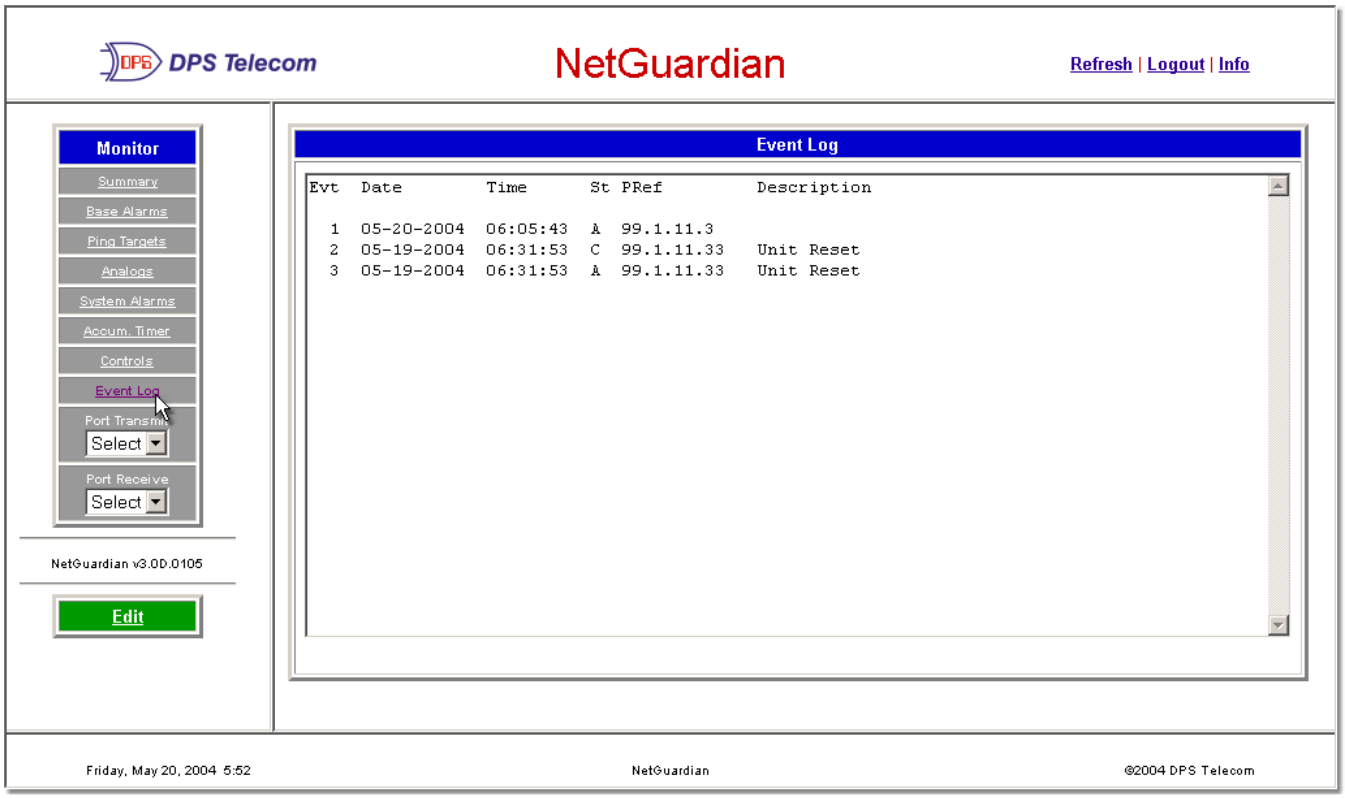


Fig. 3.7 Monitor the last 100 events recorded by the NetGuardian in the Event Log window.

Event Log Field	Description
Evt	Event number (1-100)
Date	Date the event occurred*
Time	Time the event occurred*
St	State of the event (A=alarm, C=clear)
Pref	Point reference. See Appendix A for display descriptions.
Description	User defined description of the event as entered in the alarm point and relay description fields

Table 3.A Event Logging window field descriptions.

* DCP(x) versions of the NetGuardian automatically timestamp events before sending them to the event logs. The time is based on the real-time clock (if installed) or if no real-time clock is installed, the time is based on the NetGuardian's software clock (requires resetting after power failure or power cycle).

3.8 Monitoring Data Port Activity

The Port Transmit and Port Receive windows provide live status information for the eight data ports by displaying transmit or receive activity in ASCII for the selected port. See Appendix C, ASCII Conversion, for specific ASCII symbol conversion.

Fig. 3.8 Monitor live data from your NetGuardian via the Monitor > Port Receive drop-down menu.

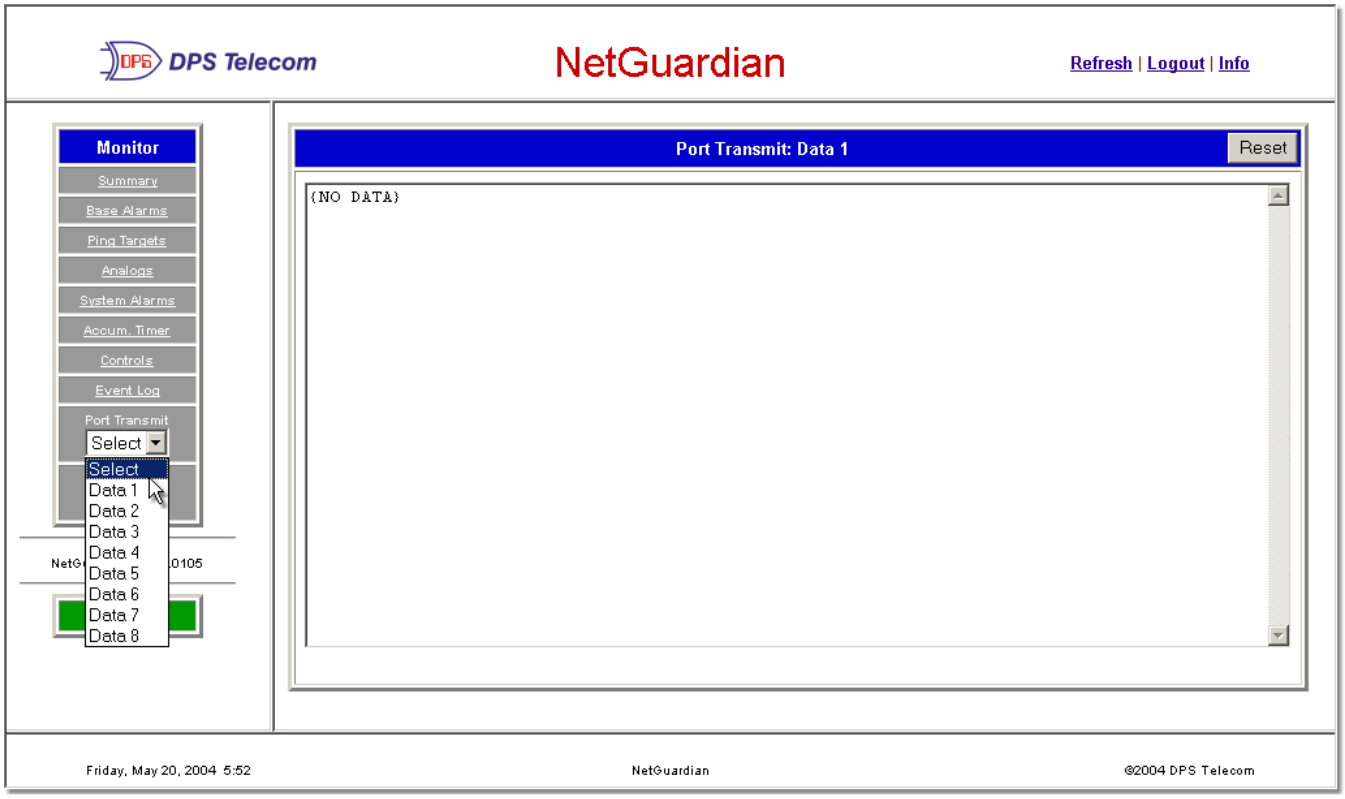


Fig. 3.9 Monitor live data being transferred from your equipment.

To view the data transmitting from the connected equipment, select the receive queue from the NetGuardian. To view the data being received by the connected equipment, select the transmit queue from the NetGuardian via the

Monitor Menu > Port Transmit drop-down menu.

3.9 Monitoring Camera Activity

In order to view camera activity via the Web Browser, you must configure your camera options in the NGEdit utility first—refer to the NGEdit user manual for details.

Select the Site Camera drop-down menu from the Monitor menu to view activity from the site camera. Bandwidth usage in live streaming mode is rated at 146kB per second.

Note: The NetGuardian only sends the camera data when a user is monitoring the image.

Fig. 3.10 Monitor live streaming video via the NetGuardian's web browser.

3.9.1 Pan-and-tilt Camera Controls

Control left-right and up-down viewing options via the Pan/Tilt options. Clicking on the image will make that the new center point.
Note: In order to have pan-and-tilt controls your Internet settings must be set to check for newer versions of stored pages every visit to the page.

Fig. 3.11 Use the arrow buttons to use the pan-and-tilt features of the NetGuardian SiteCAM.

The Preset number controls allow you to tilt to the four corners of the screen (1-4). To alter the screen size click on the Program link . To adjust the brightness, click on the – to darken the image screen or + to brighten it. Click on STD to return to the default settings.

3.9.2 Monitoring Multiple Cameras

You can monitor multiple cameras at one time by clicking the Multiple link. To view individual screens you may select the site camera under the monitor menu, or click on the title of the screen you wish to view individually. To view multiple camera activity click on the Setup-Multiple link—see Figure 3.12. To configure your multiple camera settings, click on the Setup-Multiple link—see Figure 3.13

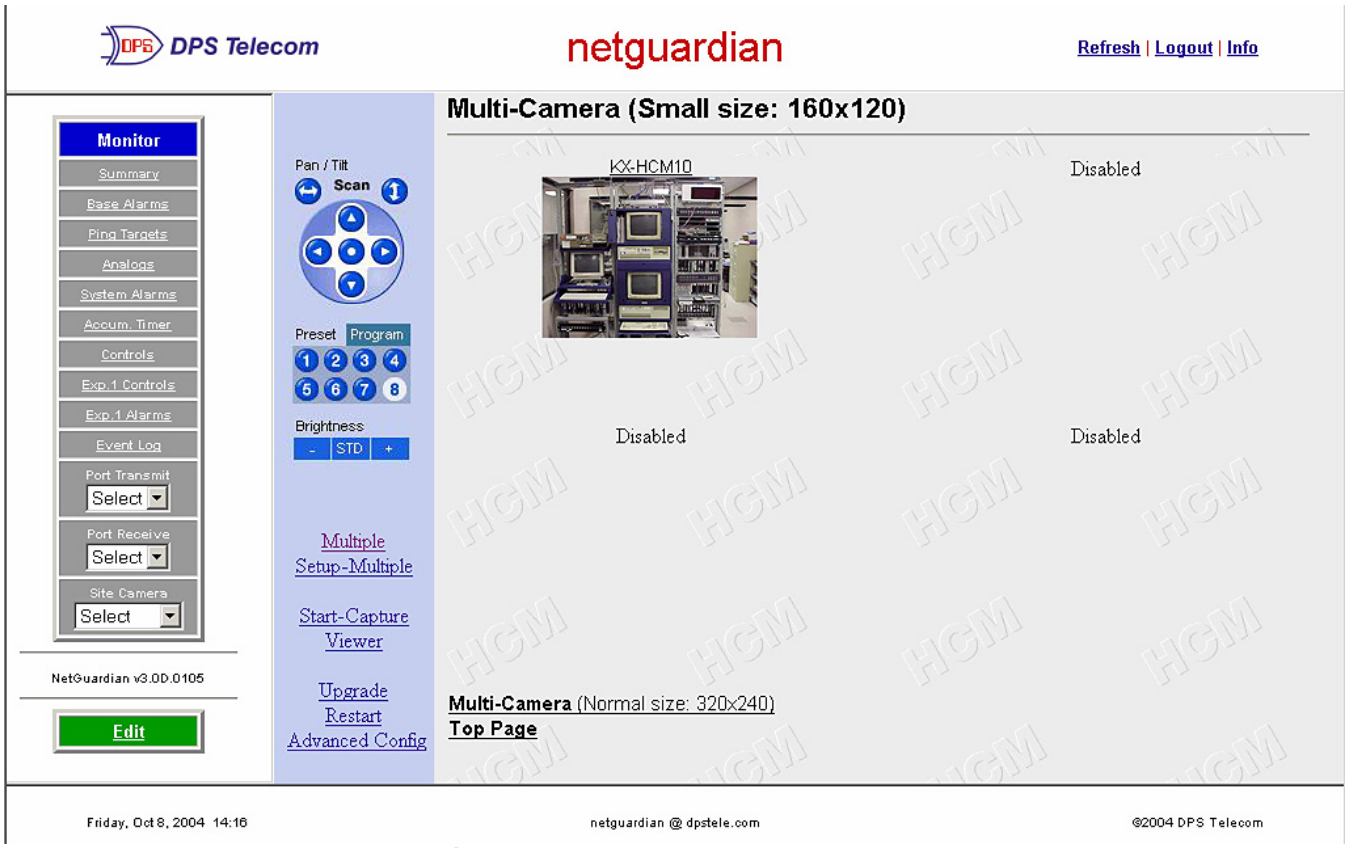


Fig. 3.12 View up to 4 multiple cameras.

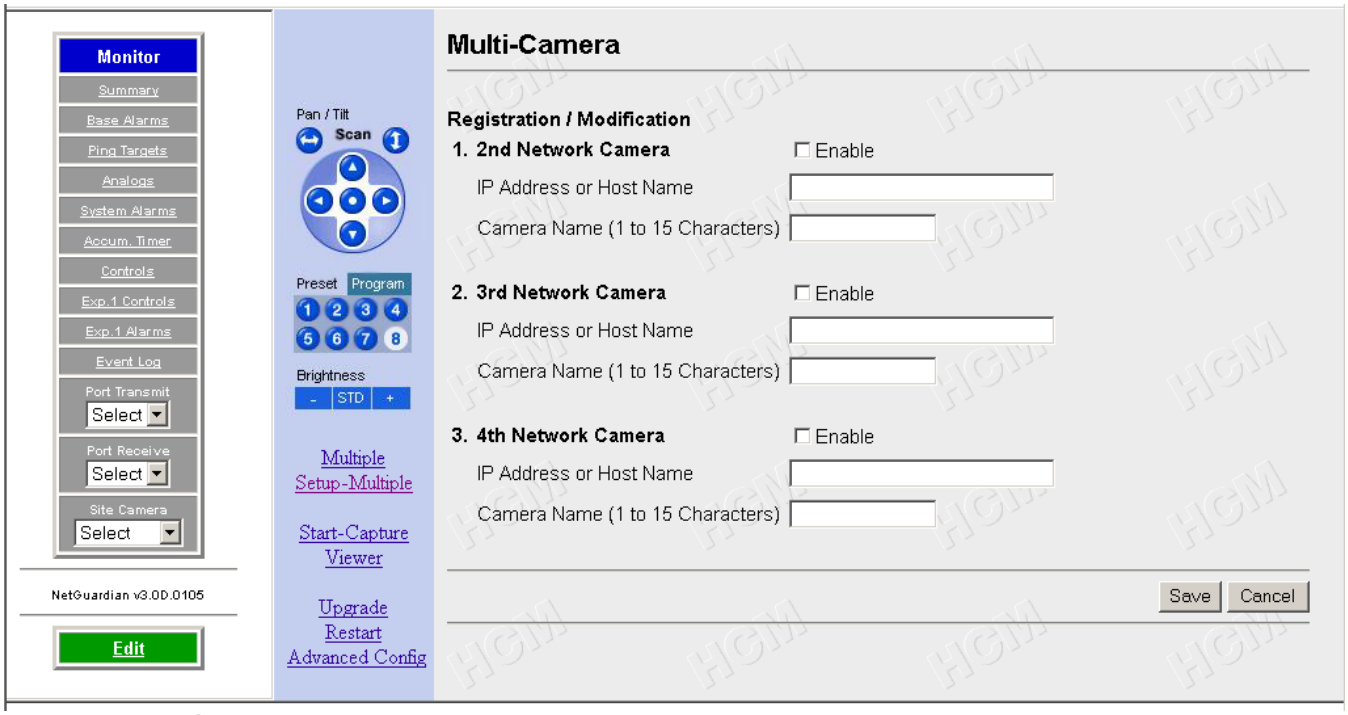


Fig. 3.13 Enter the IP Address or Host Name of each camera, and title your camera.

Before you can setup multiple camera views, you will need to set up your camera for "live streaming." See your camera user manual to configure your camera for live streaming. You may only use up to 15 alphanumeric characters to name your camera. Once you have finished click the save button.

4 Appendices

4.1 Display Mapping Appendix A

Port	Address	Display	Description	Set	Clear
99	1	1	Discrete Alarms 1-32	8001-8032	9001-9032
99	1	2	Ping Table	8065-8096	9065-9096
99	1	3	Analog Channel 1**	8129-8132	9129-9132
99	1	4	Analog Channel 2**	8193-8196	9193-9196
99	1	5	Analog Channel 3**	8257-8260	9257-9260
99	1	6	Analog Channel 4**	8321-8324	9321-9324
99	1	7	Analog Channel 5**	8385-8388	9385-9388
99	1	8	Analog Channel 6**	8449-8452	9449-9452
99	1	9	Analog Channel 7**	8513-8516	9513-9516
99	1	10	Analog Channel 8**	8577-8580	9577-9580
99	1	11	Relays/System Alarms (See Table A2)	8641-8674	9641-9674

Table A1 Display descriptions and SNMP Trap numbers for the NetGuardian.

* The TRAP number ranges shown correspond to the point range of each display. For example, the SNMP Trap "Set" number for alarm 1 (in Display 1) is 8000, "Set" for alarm 2 is 8001, "Set" for alarm 3 is 8002, etc.
** The TRAP number descriptions for the Analog channels (1-8) are in the following order: minor under, minor

over, major under, and major over. For example, for Analog channel 1, the "Set" number for minor under is 8128, minor over is 8129, major under is 8130, and major over is 8131.

		SNMP Trap #s	
Points	Description	Set	Clear
1	Relays	8641	9641
2	Relays	8642	9642
3	Relays	8643	9643
4	Relays	8644	9644
5	Relays	8645	9645
6	Relays	8646	9646
7	Relays	8647	9647
8	Relays	8648	9648
17	Timed Tick	8657	9657
18	Exp. Module Callout	8658	9658
19	Network Time Server	8659	9659
20	Accumulation Event	8660	9660
21	Duplicate IP Address	8661	9661
33	Power up	8673	9673
36	Lost Provisioning	8676	9676
37	DCP Poller Inactive	8677	9677
38	LAN not active	8678	9678
41	Modem not responding	8681	9681
42	No Dial Tone	8682	9682
43	SNMP Trap not Sent	8683	9683
44	Pager Que Overflow	8684	9684
45	Notification failed	8685	9685
46	Craft RcvQ full	8686	9686
47	Modem RcvQ full	8687	9687
48	Serial 1 RcvQ full	8688	9688
49	Serial 2 RcvQ full	8689	9689
50	Serial 3 RcvQ full	8690	9690
51	Serial 4 RcvQ full	8691	9691
52	Serial 5 RcvQ full	8692	9692
53	Serial 6 RcvQ full	8693	9693
54	Serial 7 RcvQ full	8694	9694
55	Serial 8 RcvQ full	8695	9695
56	NetGuardian DX 1 fail	8696	9696
57	NetGuardian DX 2 fail	8697	9697
58	NetGuardian DX 3 fail	8698	9698
59	GLD 1 fail	8699	9699
60	GLD 2 fail	8700	9700
61	GLD 3+ fail	8701	9701
62	Chan. Port Timeout	8702	9702
63	Craft Timeout	8703	9703
64	Event Que Full	8704	9704

Table A2 Display 11 System Alarms point descriptions.

4.2 SNMP Manager Functions Appendix B

The SNMP Manager allows the user to view alarm status, set date/time, issue controls, and perform a resync. The display and tables below outline the MIB object identifiers. Figure 1 begins with dpsRTU, however, the MIB object identifier tree has several levels above it. The full English name is as follows: root.iso.org.dod.internet.private.enterprises.dps-Inc.dpsAlarmControl.dpsRTU. Therefore, dpsRTU's full object identifier is 1.3.6.1.4.1.2682.1.2. Each level beyond dpsRTU adds another object identifying number. For example, the object identifier of the Display portion of the ControlGrid is 1.3.6.1.4.1.2682.1.2.3.3 because the object identifier of dpsRTU is 1.3.6.1.4.1.2682.1.2 + the ControlGrid (.3) + the Display (.3).

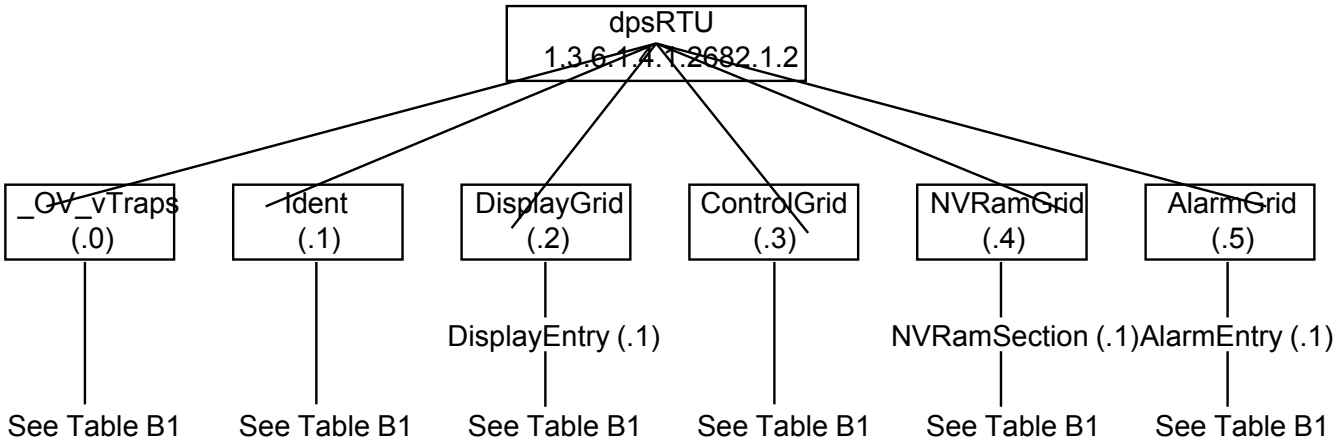


Table B1 - _OV_vTraps points.

Table B2 - Identity points.

Ident (1.3.6.1.4.1.2682.1.2.1)
Manufacturer (.1)
Model (.2)
Firmware Version (.3)
DateTime (.4)
ResyncReq (.5)*

* Must be set to "1" to perform the resync request which will resend TRAPs for any standing alarm.

Table B3 - DisplayGrid points.

DisplayEntry (1.3.6.1.4.1.2682.1.2.2.1)
Port (.1)
Address (.2)
Display (.3)
DispDesc (.4)*
PntMap (.5)*

* For specific Display and PntMap descriptions see table A1.

Table B4 - ControlGrid points.

Table B5 - NVRamSection points.

Table B6 - AlarmEntry points.

AlarmEntry (1.3.6.4.1.2682.1.2.5.1)
APort (.1)
AAddress (.2)
ADisplay (.3)
APoint (.4)
APntDesc (.5)*
AState (.6)

* For specific point descriptions, see table B7.

	Description	Port	Address	Display	Points
Disp 1	No data*	99	1	1	1-32
	Undefined**	99	1	1	33-64
Disp 2	No data*	99	1	2	1-32
	Undefined**	99	1	2	33-64
Disp 3	Analog 1	99	1	3	1-4
	Undefined**	99	1	3	5-64
Disp 4	Analog 2	99	1	4	1-4
	Undefined**	99	1	4	5-64
Disp 5	Analog 3	99	1	5	1-4
	Undefined**	99	1	5	5-64
Disp 6	Analog 4	99	1	6	1-4
	Undefined**	99	1	6	5-64
Disp 7	Analog 5	99	1	7	1-4
	Undefined**	99	1	7	5-64
Disp 8	Analog 6	99	1	8	1-4
	Undefined**	99	1	8	5-64
Disp 9	Analog 7	99	1	9	1-4
	Undefined**	99	1	9	5-64
Disp 10	Analog 8	99	1	10	1-4
	Undefined**	99	1	10	5-64
Disp 11	No data*	99	1	11	1-8
	Undefined**	99	1	11	9-32
	Power up	99	1	11	33
	Undefined**	99	1	11	34-35
	Lost	99	1	11	36
	DCP poll inactive	99	1	11	37
	LAN not active	99	1	11	38
	Undefined**	99	1	11	39-40
	Modem not	99	1	11	41
	No dial-tone	99	1	11	42
	SNMP trap not	99	1	11	43
	Pager Que	99	1	11	44
	Notification	99	1	11	45
	Craft RCVQ full	99	1	11	46
	Modem RCVQ	99	1	11	47
	Data 1-8 RCVQ	99	1	11	48-55
	NGdx 1-3 fail	99	1	11	56-58
	GLD 1-3 fail	99	1	11	59-61
	CHAN timeout	99	1	11	62
	CRFT timeout	99	1	11	63

Table B7 Alarm Point Descriptions.

* "No data" indicates that the alarm point is defined but there is no description entered.
** "Undefined" indicates that the alarm point is not used.

4.3 SNMP Granular Trap Packets Appendix C

Tables C and C1 provide a list of the information contained in the SNMP Trap packets sent by the NetGuardian. SNMP Trap managers can use 1 of 2 methods to get alarm information: 1. - Granular traps (not necessary to define point descriptions for the NetGuardian) or 2. - The SNMP manager reads the description from the Trap.

UDP Header	Description
1238	Source port
162	Destination port
303	Length
0xBAB0	Checksum

Table C1 UDP Headers and descriptions.

SNMP Header	Description
0	Version
public	Request
Trap	Request
1.3.6.1.4.1.2682.1.2	Enterprise
126.10.230.181	Agent address
Enterprise Specific	Generic Trap
8001	Specific Trap
617077	Time stamp
1.3.7.1.2.1.1.1.0	Object
NetGuardian v.2.5.140	Value
1.3.6.1.2.1.1.6.0	Object
1-800-622-3314	Value
1.3.6.1.4.1.2682.1.2.4.1.0	Object
01-02-1995 05:08:27.760	Value
1.3.6.1.4.1.2682.1.2.5.1.1.99.1.1.1	Object
99	Value
1.3.6.1.4.1.2682.1.2.5.1.2.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.2.5.1.3.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.2.5.1.4.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.2.5.1.5.99.1.1.1	Object
Rectifier Failure	Value
1.3.6.1.4.1.2682.1.2.5.1.6.99.1.1.1	Object
Alarm	Value

Table C2 SNMP Headers and descriptions.

4.4 ASCII Conversion Appendix D

The information contained in Table D is a list of ASCII symbols and their meanings. Refer to the bulleted list below to interpret the ASCII data transmitted or received through the data ports. Port transmit and receive activity can be viewed from the Web Browser interface.

- Printable ASCII characters will appear as ASCII.
- Non-printable ASCII characters will appear as labels surrounded by { } brackets (e.g. {NUL}).
- Non-ASCII characters will appear as hexadecimal surrounded by [ ] brackets (e.g. [IF]).
- A received BREAK will appear as <BRK>.

Abbreviation	Description	Abbreviation	Description
NUL	Null	DLE	Data Link Escape
SOH	Start of Heading	DC	Device Control
STX	Start of Text	NAK	Negative Acknowledge
ETX	End of Text	SYN	Synchronous Idle
EOT	End of Transmission	ETB	End of Transmission Block
ENQ	Enquiry	CAN	Cancel
ACK	Acknowledge	EM	End of Medium
BEL	Bell	SUB	Substitute
BS	Backspace	ESC	Escape
HT	Horizontal Tabulation	FS	File Separator
LF	Line Feed	GS	Group Separator
VT	Vertical Tabulation	RS	Record Separator
FF	Form Feed	US	Unit Separator
CR	Carriage Return	SP	Space (blank)
SO	Shift Out	DEL	Delete
SI	Shift In	BRK	Break Received

Table D ASCII symbols.

4.5 System Alarms Display Map

Display	Points	Alarm Point	Description	Solution
11	17	Timed Tick	Toggles state at constant rate as configured by the Timed Tick timer variable. Useful in testing integrity of SNMP trap alarm reporting.	To turn the feature off, set the Timed Tick timer to 0.
	18	Exp. Module Callout	Alarm is triggered whenever an alarm point from an Entry Control Unit (ECU) is collected. A notification event may be associated with the alarm to force a call out or trap.	Disable Building Access Control (BAC) by setting the BAC Unit ID to 0. If Building Access is being used, then investigate the ECU alarm source or don't associate notification with the alarm event.
	19	Network Time Server	Communication with Network Time Server has failed.	Try pinging the Network Time Server's IP Address as it is configured. If the ping test is successful, then check the port setting and verify the port is not being blocked on your network.
	20	Accumulation Event	An alarm has been standing for the time configured under Accum. Timer. The Accumulation timer enables you to monitor how long an alarm has been standing despite system reboots. Only the user may reset the accumulated time, a reboot will not.	To turn off the feature, under Accum.Timer, set the display and point reference to 0.
	21	Duplicate IP Address	The unit has detected another node with the same IP Address.	Unplug the LAN cable and contact your network administrator. Your network and the unit will most likely behave incorrectly. After assigning a correct IP Address, reboot the unit to clear the System alarm.
	33	Power up	The unit has just come-online. The set alarm condition is followed immediately by a clear alarm condition.	Seeing this alarm is normal if the unit is powering up.
	36	Lost Provisioning	The internal NVRAM may be damaged. The unit is using default configuration settings.	Use Web or latest version of NGEdit to configure unit. Power cycle to see if alarm goes away. May require RMA.

Table E1 System Alarms Descriptions

Display	Points	Alarm Point	Description	Solution
11	37	DCP Poller Inactive	The unit has not seen a poll from the Master for the time specified by the DCP Timer setting.	If DCP responder is not being used, then set the DCP Unit ID to 0. Otherwise, try increasing the DCP timer setting under timers, or check how long it takes to cycle through the current polling chain on the Master system.
	38	LAN not active	The 10bt LAN port is down.	Check LAN cable. Ping to and from the unit.
	41	Modem not responding	An error has been detected during modem initialization. The modem did not respond to the initialization string.	Remove configured modem initialization string, then power cycle the unit. If alarm persists, try resetting the Modem port from the TTY interface, or contact DPS for possible RMA.
	42	No Dial Tone	During dial-out attempt, the unit did not detect a dial tone.	Check the integrity of the phone line and cable.
	43	SNMP Trap not Sent	SNMP trap address is not defined and an SNMP trap event occurred.	Define the IP Address where you would like to send SNMP trap events, or configure the event not to trap.
	44	Pager Que Overflow	Over 250 events are currently queued in the pager queued and are still trying to report.	Check for failed notification events that may be filling up the pager queue. There may be a configuration or communication problem with the notification events.
	45	Notification failed	A notification event, like a page or email, was unsuccessful.	Use RPT filter debug to help diagnose notification problems.
	46	Craft RcvQ full	The Craft port received more data than it was able to process.	Disconnect whatever device is connected to the craft serial port. This alarm should not occur.
	47	Modem RcvQ full	The modem port received more data than it was able to process.	Check what is connecting to the NetGuardian. This alarm should not occur.
	48	Serial 1 RcvQ full	Serial port 1 (or appropriate serial port number) receiver filled with 8 K of data (4 K if BAC active).	Check proxy connection. The serial port data may not be getting collected as expected.
	49	Serial 2 RcvQ full		
	50	Serial 3 RcvQ full		
	51	Serial 4 RcvQ full		
	52	Serial 5 RcvQ full		
	53	Serial 6 RcvQ full		
	54	Serial 7 RcvQ full		
	55	Serial 8 RcvQ full		

Table E1 System Alarms Descriptions (continued)

Display	Points	Alarm Point	Description	Solution
11	56	NetGuardian DX 1 fail	NGDdx 1 Fail (Expansion shelf 1 communication link failure)	Under Ports > Options, verify the number of configured NGDdx units. Use EXP filter debug and port LEDs to help diagnose the problem. Use DB9M to DB9M with null crossover for cabling. Verify the DIP addressing on the back of the NGDdx unit.
	57	NetGuardian DX 2 fail	NGDdx 2 Fail (Expansion shelf 2 communication link failure)	
	58	NetGuardian DX 3 fail	NGDdx 3 Fail (Expansion shelf 3 communication link failure)	
	59	GLD 1 fail	GLD address 1 is failed.	Connect just GLD unit 1 and attempt to poll. Verify GLD is connected to data port 8 and the hardware is RS485, not RS232.
	60	GLD 2 fail	GLD address 2 is failed.	Verify the GLD unit addressing, and test GLD units individually on the GLD communication bus.
	61	GLD 3+ fail	One or more GLD units addressed 3 through 12 may be failed.	Reduce the number of connected GLD units to determine which unit may be causing the link to fail.
	62	Chan. Port Timeout	Chan. Port has not forwarded any traffic in the time specified by the Channel Timeout Timer. The channel feature forwards data between two ports so the NG may be used to analyze serial traffic using CHAN filter debug.	Change the data port type to OFF, or set the Channel Timer to a different setting.
	63	Craft Timeout	The Craft Timeout Timer has not been reset in the specified time. This feature is designed so other machines may keep the TTY link active. If the TTY interface becomes unavailable to the machine, then the Craft Timeout alarm is set.	Change the Craft Timeout Timer to 0 to disable the feature.
	64	Event Que Full	The Event Que is filled with more than 500 uncollected events.	Enable DCP timestamp polling on the master so events are collected, or reboot the system to clear the alarm.

Table E1 System Alarms Descriptions (continued)

5 Frequently Asked Questions

5.1 General FAQs

Q. How do I Telnet to the NetGuardian?
A. You must use **Port 2002** to connect to the NetGuardian. Configure your Telnet client to connect using TCP/IP (**not** Telnet, or any other port options). For connection information, enter the IP address of the NetGuardian and Port 2002. For example, to connect to the NetGuardian using the standard Windows Telnet client, click Start, click Run, and type Telnet <NetGuardian IP address> 2002.

Q. How can I back up the current configuration of my NetGuardian?
A. There are two ways. NGEdit can read the configuration of your NetGuardian and save the configuration to your PC's hard disk or a floppy disk. With NGEdit you can also make changes to the configuration file and write the changed configuration to the NetGuardian's NVRAM. The other way is to use File Transfer Protocol (FTP). You can use FTP to read configuration files from or write files to the NetGuardian's NVRAM, but you can't use FTP to edit configuration files.

Q. Can I use my NetGuardian as a proxy server to access TTY interfaces on my third-party serial equipment?
A. You can use Data Ports 1–8, located on the back of the NetGuardian, to connect to serial devices, as long as your devices support RS-232. To make a proxy connection, you must define the correct TCP port for each serial port. To define TCP ports, you must first connect directly to the NetGuardian through its IP address. Once you have connected to the NetGuardian, you can define the TCP ports through the NetGuardian's TTY or Web Browser configuration interfaces.

Q. What do the terms alarm point, display, port, and address mean?
A. These terms define the exact location of a network alarm, from the most specific (an individual alarm point) to the most general (an entire monitored device). An alarm point is a number representing an actual contact closure that is activated when an alarm condition occurs. For example, an alarm point might represent a low oil sensor in a generator or a open/closed sensor in a door. A display is a logical group of 64 alarm points. A port is traditionally the actual physical serial port through which the monitoring device collects data. The address is a number representing the monitored device. The terms port and address have been extended to refer to logical, or virtual, ports and addresses. For example, the NetGuardian reports internal alarms on Port 99, address 1.

Q. What characteristics of an alarm point can I configure through software? For instance, can I configure Point 4 to sense an active-low (normally closed) signal, or Point 5 to sense a level or edge?
A. The NetGuardian alarm points are level sensed and can be software-configured to generate an alarm on either a high (normally open) or low (normally closed) level.

Q. When I connect to the NetGuardian through the craft port on the front panel it either doesn't work right or it doesn't work at all. What's going on?
A. Make sure your using the right COM port settings. The standard settings for the craft port are 9600 baud, 8 bits, no parity, and 1 stop bit. Flow control **must** be set to **none**. Flow control normally defaults to hardware in most terminal programs, and this will not work correctly with the NetGuardian.

Q. I just changed the port settings for one of my data ports, but the changes did not seem to take effect even after I wrote the NVRAM.
A. In order for data port and craft port changes (including changes to the baud rate and word format) to take effect, the NetGuardian must be rebooted. Whenever you make changes, remember to write them to the NetGuardian's NVRAM so they will be saved when the unit is rebooted.

Q. How do I get my NetGuardian on the network?

A. Before the NetGuardian will work on your LAN, the unit address (IP address), the subnet mask, and the default gateway must be set. A sample configuration could look like this:

unit address: 192.168.1.100
subnet mask: 255.255.255.0
Default Gateway: 192.168.1.1

Always remember to save your changes by writing to the NVRAM. Any modifications of the NetGuardian's IP configuration will also require a reboot.

Q. Does the PPP allow upload of new firmware over PPP?
A. The NetGuardian supports all PPP upload capabilities with the exception of firmware.

Q. I'm using HyperTerminal to connect to the NetGuardian through the craft port, but the unit won't accept input when I get to the first level menu.
A. Make sure you turn off all handshaking in HyperTerminal.

Q. I can't change the craft port baud rate.
A. Once you select a higher baud rate, you must set your terminal emulation to that new baud rate and enter the DPSCFG and press Enter escape sequence. The craft port interprets a break key as an override to 9600 baud. At slower baud rates, normal keys can appear as a break.

Q. The LAN line LED is green on my NetGuardian, but I can't poll it from my T/MonXM master.
A. Some routers will not forward to an IP address until the MAC address has been registered with the router. You need to enter the IP address of your T/MonXM system or your gateway in the ping table.

5.2 SNMP FAQs

Q. Which version of SNMP is supported by the SNMP agent on the NetGuardian?
A. SNMP v1.

Q. How do I configure the NetGuardian to send traps to an SNMP manager? Is there a separate MIB for the NetGuardian? How many SNMP managers can the agent send traps to? And how do I set the IP address of the SNMP manager and the community string to be used when sending traps?
A. The NetGuardian begins sending traps as soon as the SNMP managers are defined. The NetGuardian MIB is included on the NetGuardian Resource CD. The MIB should be compiled on your SNMP manager. (Note: MIB versions may change in the future.) The unit supports a main SNMP manager, which is configured by entering its IP address in the trap address field of Ethernet Port Setup. You can also configure up to eight secondary SNMP managers, which is configured by selecting the secondary SNMP managers as pager recipients. Community strings are configured globally for all SNMP managers. To configure the community strings, choose System from the Edit menu, and enter appropriate values in the Get, Set, and Trap fields.

Q. Does the NetGuardian support MIB-2 and/or any other standard MIBs?
A. The NetGuardian supports the bulk of MIB-2.

Q. Does the NetGuardian SNMP agent support both NetGuardian and T/MonXM variables?
A. The NetGuardian SNMP agent manages an embedded MIB that supports only the NetGuardian's RTU variables. The T/MonXM variables are included in the distributed MIB only to provide SNMP managers with a single MIB for all DPS Telecom products.

Q. How many traps are triggered when a single point is set or cleared? The MIB defines traps like major alarm set/cleared, RTU point set, and a lot of granular traps, which could imply that more than one trap is sent when a change of state occurs on one point.
A. Generally, a single change of state generates a single trap, but there are two exception to this rule. Exception 1: the first alarm in an all clear condition generates an additional summary point set trap.

Exception 2: the final clear alarm that triggers an all clear condition generates an additional summary point clear trap.

Q. What does point map mean?
A. A point map is a single MIB leaf that presents the current status of a 64-alarm-point display in an ASCII-readable form, where a "."represents a clear and an "x" represents an alarm.

Q. The NetGuardian manual talks about eight control relay outputs. How do I control these from my SNMP manager?
A. The control relays are operated by issuing the appropriate set commands, which are contained in the DPS Telecom MIB. For more information about the set commands, see Reference Information, Display Mapping, in any of the NetGuardian software configuration guides.

Q. How can I associate descriptive information with a point for the RTU granular traps?
A. The NetGuardian alarm point descriptions are individually defined using the Web Browser, TTY, or NGEdit configuration interfaces.

Q. My SNMP traps aren't getting through. What should I try?
A. Try these three steps:

1. Make sure that the trap address (IP address of the SNMP manager) is defined. (If you changed the trap address, make sure you saved the change to NVRAM and rebooted.)
2. Make sure all alarm points are configured to send SNMP traps.
3. Make sure the NetGuardian and the SNMP manager are both on the network. Use the NetGuardian's ping command to ping the SNMP manager.

5.3 Pager FAQs

Q. Why won't my alpha pager work?
A. To configure the NetGuardian to send alarm notifications to an alpha pager, enter the **data** phone number for your pager in the Phone Number field. This phone number should connect to your pager services modem. Then enter the PIN for your pager in the PIN/Rcpt/Port field. You don't need to enter anything in any of the other fields. If you still don't receive pages, try setting the Dial Modem Init string to ATS37=9. This will limit the NetGuardian's connection speed.

Q. Numeric pages don't come in or are cut off in the middle of the message. What's wrong?
A. You need to set a delay between the time the NetGuardian dials your pager number and the time the NetGuardian begins sending the page message. You can set the delay in the Pager Number field, where you enter your pager number. First enter the pager number, then enter some commas directly after the number. Each comma represents a two-second delay. So, for example, if you wanted an eight-second delay, you would enter 555-1212,,,, in the Pager Number field.

Q. What do I need to do to set up email notifications?
A. You need to assign the NetGuardian an email address and list the addresses of email recipients. Let's explain some terminology. An email address consists of two parts, the user name (everything before the @ sign) and the domain (everything after the @ sign). To assign the NetGuardian an email address, choose System from the Edit menu. Enter the NetGuardian's user name in the Name field (it can't include any spaces) and the domain in the Location field. For example, if the system configuration reads:

Name: netguardian
Location: proactive.com

Then email notifications from the NetGuardian will be sent from the address netguardian@proactive.com.
The next step is to list the email recipients. Choose Pagers from the Edit menu. For each email recipient, enter his or her email domain in the Phone/Domain field and his or her user name in the PIN/Rcpt/Port field. You must also enter the IP address of an SNMP server in the IPA field.

6 Technical Support

DPS Telecom products are backed by our courteous, friendly Technical Support representatives, who will give you the best in fast and accurate customer service. To help us help you better, please take the following steps before calling Technical Support:

1. **Check the DPS Telecom website.**
   You will find answers to many common questions on the DPS Telecom website, at **http://www.dpstele.com/support/**. Look here first for a fast solution to your problem.
2. **Prepare relevant information.**
   Having important information about your DPS Telecom product in hand when you call will greatly reduce the time it takes to answer your questions. If you do not have all of the information when you call, our Technical Support representatives can assist you in gathering it. Please write the information down for easy access. Please have your user manual and hardware serial number ready.
3. **Have access to troubled equipment.**
   Please be at or near your equipment when you call DPS Telecom Technical Support. This will help us solve your problem more efficiently.
4. **Call during Customer Support hours.** Customer support hours are Monday through Friday, from 7 A.M. to 6 P.M., Pacific time. The DPS Telecom Technical Support phone number is **(559) 454-1600**.

Emergency Assistance: *Emergency assistance is available 24 hours a day, 7 days a week. For emergency assistance after hours, allow the phone to ring until it is answered with a paging message. An on-call technical support representative will return your call as soon as possible.*

Warranty

DPS Telecom warrants, to the original purchaser only, that its products a) substantially conform to DPS' published specifications and b) are substantially free from defects in material and workmanship. This warranty expires two years from the date of product delivery with respect to hardware and ninety days from the date of product delivery with respect to software. If the purchaser discovers within these periods a failure of the product to substantially conform to the specifications or that the product is not substantially free from defects in material and workmanship, the purchaser must promply notify DPS. Within reasonable time after notification, DPS will endeavor to correct any substantial non-conformance with the specifications or substantial defects in material and workmanship, with new or used replacement parts. All warranty service will be performed at the company's office in Fresno, California, at no charge to the purchaser, other than the cost of shipping to and from DPS, which shall be the responsiblity of the purchaser. If DPS is unable to repair the product to conform to the warranty, DPS will provide at its option one of the following: a replacement product or a refund of the purchase price for the non-conforming product. These remedies are the purchaser's only remedies for breach of warranty. Prior to initial use the purchaser shall have determined the suitability of the product for its intended use. DPS does not warrant a) any product, components or parts not manufactured by DPS, b) defects caused by the purchaser's failure to provide a suitable installation environment for the product, c) damage caused by use of the product for purposes other than those for which it was designed, d) damage caused by disasters such as fire, flood, wind or lightning unless and to the extent that the product specification provides for resistance to a defined disaster, e) damage caused by unauthorized attachments or modifications, f) damage during shipment from the purchaser to DPS, or g) any abuse or misuse by the purchaser.

THE FOREGOING WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In no event will DPS be liable for any special, incidental, or consequential damages based on breach of warranty, breach of contract, negligence, strict tort, or any other legal theory. Damages that DPS will not be responsible for include but are not limited to, loss of profits; loss of savings or revenue; loss of use of the product or any associated equipment; cost of capital; cost of any substitute equipment, facilities or services; downtime; claims of third parties including customers; and injury to property.

The purchaser shall fill out the requested information on the Product Warranty Card and mail the card to DPS. This card provides information that helps DPS make product improvements and develop new products.

For an additional fee DPS may, at its option, make available by written agreement only an extended warranty providing an additional period of time for the applicability of the standard warranty.

Technical Support

If a purchaser believes that a product is not operating in substantial conformance with DPS' published specifications or there appear to be defects in material and workmanship, the purchaser should contact our technical support representatives. If the problem cannot be corrected over the telephone and the product and problem are covered by the warranty, the technical support representative will authorize the return of the product for service and provide shipping information. If the product is out of warranty, repair charges will be quoted. All non-warranty repairs receive a 90-day warranty.

Free Tech Support is Only a Click Away

Need help with your alarm monitoring? DPS Information Services are ready to serve you … in your email or over the Web!

www.DpsTelecom.com

Free Tech Support in Your Email: The Protocol Alarm Monitoring Ezine

The Protocol Alarm Monitoring Ezine is your free email tech support alert, delivered directly to your in-box every two weeks. Every issue has news you can use right away:

- Expert tips on using your alarm monitoring equipment — advanced techniques that will save you hours of work
- Educational White Papers deliver fast informal tutorials on SNMP, ASCII processing, TL1 and other alarm monitoring technologies
- New product and upgrade announcements keep you up to date with the latest technology
- Exclusive access to special offers for DPS Telecom Factory Training, product upgrade offers and discounts

To get your free subscription to The Protocol register online at
www.TheProtocol.com/register

Free Tech Support on the Web: MyDPS

MyDPS is your personalized, members-only online resource. Registering for MyDPS is fast, free, and gives you exclusive access to:

- Firmware and software downloads and upgrades
- Product manuals
- Product datasheets
- Exclusive user forms

DPS Telecom
"Your Partners in Network Alarm Monitoring"

Register for MyDPS online at
www.DpsTelecom.com/register

(800) 622-3314 • www.DpsTelecom.com • 4955 E. Yale Avenue, Fresno, California 93727